# sysmocom

sysmocom - s.f.m.c. GmbH



# OsmoSGSN User Manual

by Harald Welte and Alexander Couzens

DRAFT

Copyright © 2013-2024 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 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".

The Asciidoc source code of this manual can be found at https://git.osmocom.org/osmo-gsm-manuals/

| HISTORY | | | |
|---|---|---|---|
| NUMBER | DATE | DESCRIPTION | NAME |
| 1 | January 13, 2013 | Initial version. | HW |
| 2 | February 2016 | Conversion to asciidoc, removal of sysmoBTS specific parts. | HW |
| 3 | April 2024 | Replace NS chapter with new NS2 chapter to match the code. | AC |

Copyright © 2013-2024 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 OsmoSGSN . . . 5
4.2 Software Components . . . 5
4.2.1 Gb Implementation . . . 5
4.2.2 GTP Implementation . . . 6
4.2.3 GMM Implementation . . . 6
4.2.4 LLC Implementation . . . 6
4.2.5 Session Management Implementation . . . 6
4.3 Limitations . . . 6

**5 Running OsmoSGSN** **6**
5.1 SYNOPSIS . . . 6
5.2 OPTIONS . . . 7

**6 Control interface** **7**
6.1 subscriber-list-active-v1 . . . 7

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**7 The Osmocom VTY Interface 7**
7.1 Accessing the telnet VTY . . . 9
7.2 VTY Nodes . . . 9
7.3 Interactive help . . . 9
7.3.1 The question-mark (?) command . . . 10
7.3.2 TAB completion . . . 11
7.3.3 The list command . . . 11
7.3.4 The attribute system . . . 13
7.3.5 The expert mode . . . 14

**8 libosmocore Logging System 15**
8.1 Log categories . . . 15
8.2 Log levels . . . 15
8.3 Log printing options . . . 16
8.4 Log filters . . . 16
8.5 Log targets . . . 17
8.5.1 Logging to the VTY . . . 17
8.5.2 Logging to the ring buffer . . . 17
8.5.3 Logging via gsmtap . . . 17
8.5.4 Logging to a file . . . 19
8.5.5 Logging to syslog . . . 19
8.5.6 Logging to systemd-journal . . . 20
8.5.7 Logging to stderr . . . 21

**9 Configuring OsmoSGSN 21**
9.1 Configuring the Gp interface (towards GGSN) . . . 21
9.1.1 Static GGSN/APN configuration . . . 21
9.1.2 Dynamic GGSN/APN configuration . . . 22
9.2 Configuring the Gp interface (towards MME) . . . 22
9.2.1 Static MME/TAI configuration . . . 22
9.2.2 Dynamic MME/TAI configuration . . . 23
9.3 Authorization Policy . . . 23
9.4 Subscriber Configuration . . . 24
9.4.1 Accessing an external HLR via GSUP . . . 24
9.5 CDR configuration . . . 25
9.5.1 CDR CTRL interface . . . 25
9.5.2 CDR Format . . . 25
9.6 User traffic compression . . . 26
9.6.1 Header compression . . . 26
9.6.2 Data compression . . . 27
9.7 Encryption . . . 27
9.8 Configure SCCP/M3UA to accept *IuPS* links . . . 28

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**10 Configure SCCP/M3UA** **28**
10.1 Connect to STP Instance . . . 29
10.2 Local Point-Code . . . 30
10.3 Remote Point-Code . . . 30
10.4 Point-Code Format . . . 31
10.5 AS and ASP . . . 31
10.6 Subsystem Number (SSN) . . . 32
10.7 Routing Context / Routing Key . . . 32
10.7.1 M3UA without Routing Context IE / Routing Context *0* . . . 33
10.7.2 Example: Static Routing . . . 33

**11 Gb/NS Network Service** **35**
11.1 Gb interface variants . . . 35
11.1.1 Gb over Frame Relay over E1/T1 . . . 36
11.1.1.1 FR Driver Support . . . 36
11.1.2 Gb over Frame Relay encapsulated in GRE/IP . . . 36
11.1.3 Gb over IP "ip.access style" . . . 36
11.1.4 Gb over IP 3GPP static and auto-configuration . . . 37
11.1.4.1 Gb over IP 3GPP auto-configuration . . . 37
11.2 General structure . . . 38
11.2.1 bind (NS-VL) . . . 38
11.2.2 NS-E . . . 38
11.2.3 NS-VC . . . 38
11.3 Gb/NS configuration . . . 39
11.3.1 Gb over Frame Relay over E1/T1 . . . 39
11.3.2 Gb over IP "ip.access style" . . . 40
11.3.2.1 Gb over IP "ip.access style" dynamic configuration . . . 40
11.3.2.2 Gb over IP "ip.access style" static configuration . . . 41
11.3.3 Gb over IP 3GPP static configuration . . . 41
11.3.4 Gb over IP 3GPP auto configuration as BSS . . . 41
11.3.5 Gb/NS Timer configuration . . . 42
11.4 Gb/NS maintenance . . . 42
11.4.1 NSE states . . . 42
11.4.2 NSVC states . . . 43
11.4.3 Show information of a specific NSE . . . 44
11.4.4 Blocking a NSVC . . . 45

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**12 Osmocom Control Interface** **46**
12.1 Control Interface Protocol . . . 46
12.1.1 GET operation . . . 47
12.1.2 SET operation . . . 47
12.1.3 TRAP operation . . . 47
12.2 Common variables . . . 48
12.3 Control Interface python examples . . . 48
12.3.1 Getting rate counters . . . 49
12.3.2 Setting a value . . . 49
12.3.3 Getting a value . . . 49
12.3.4 Listening for traps . . . 49

**13 Osmocom Authentication Protocol (OAP)** **49**
13.1 General . . . 49
13.2 Connection . . . 50
13.3 Using IPA . . . 50
13.4 Procedures . . . 50
13.4.1 Register . . . 50
13.4.2 Challenge . . . 51
13.4.3 Challenge Result . . . 51
13.4.4 Sync Request . . . 51
13.4.5 Sync Result . . . 51
13.4.6 Register Result . . . 51
13.5 Message Format . . . 51
13.5.1 Register Request . . . 51
13.5.2 Register Error . . . 51
13.5.3 Register Result . . . 52
13.5.4 Challenge . . . 52
13.5.5 Challenge Error . . . 52
13.5.6 Challenge Result . . . 52
13.5.7 Sync Request . . . 52
13.5.8 Sync Error . . . 52
13.5.9 Sync Result . . . 52
13.6 Information Elements . . . 53
13.6.1 Message Type . . . 53
13.6.2 IE Identifier (informational) . . . 53
13.6.3 Client ID . . . 53

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**14 Generic Subscriber Update Protocol 53**
14.1 General . . . 53
14.2 Connection . . . 54
14.3 Using IPA . . . 54
14.4 Procedures . . . 54
14.4.1 Authentication management . . . 54
14.4.2 Reporting of Authentication Failure . . . 54
14.4.3 Location Updating . . . 55
14.4.4 Location Cancellation . . . 55
14.4.5 Purge MS . . . 55
14.4.6 Delete Subscriber Data . . . 56
14.4.7 Check IMEI . . . 56
14.5 Procedures (E Interface) . . . 56
14.5.1 E Handover . . . 56
14.5.2 E Subsequent Handover . . . 57
14.5.3 E Forward and Process Access Signalling . . . 57
14.5.4 E Routing Error . . . 58
14.6 Message Format . . . 58
14.6.1 General . . . 58
14.6.2 Send Authentication Info Request . . . 58
14.6.3 Send Authentication Info Error . . . 59
14.6.4 Send Authentication Info Response . . . 59
14.6.5 Authentication Failure Report . . . 59
14.6.6 Update Location Request . . . 59
14.6.7 Update Location Error . . . 59
14.6.8 Update Location Result . . . 59
14.6.9 Location Cancellation Request . . . 60
14.6.10 Location Cancellation Error . . . 60
14.6.11 Location Cancellation Result . . . 60
14.6.12 Purge MS Request . . . 60
14.6.13 Purge MS Error . . . 60
14.6.14 Purge MS Result . . . 61
14.6.15 Insert Subscriber Data Request . . . 61
14.6.16 Insert Subscriber Data Error . . . 61
14.6.17 Insert Subscriber Data Result . . . 61
14.6.18 Delete Subscriber Data Request . . . 61
14.6.19 Delete Subscriber Data Error . . . 62
14.6.20 Delete Subscriber Data Result . . . 62
14.6.21 Process Supplementary Service Request . . . 62

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

14.6.22 Process Supplementary Service Error . . . 62
14.6.23 Process Supplementary Service Response . . . 62
14.6.24 MO-forwardSM Request . . . 63
14.6.25 MO-forwardSM Error . . . 63
14.6.26 MO-forwardSM Result . . . 63
14.6.27 MT-forwardSM Request . . . 64
14.6.28 MT-forwardSM Error . . . 64
14.6.29 MT-forwardSM Result . . . 64
14.6.30 READY-FOR-SM Request . . . 64
14.6.31 READY-FOR-SM Error . . . 65
14.6.32 READY-FOR-SM Result . . . 65
14.6.33 CHECK-IMEI Request . . . 65
14.6.34 CHECK-IMEI Error . . . 65
14.6.35 CHECK-IMEI Result . . . 65
14.6.36 E Prepare Handover Request . . . 66
14.6.37 E Prepare Handover Error . . . 66
14.6.38 E Prepare Handover Result . . . 66
14.6.39 E Prepare Subsequent Handover Request . . . 66
14.6.40 E Prepare Subsequent Handover Error . . . 66
14.6.41 E Prepare Subsequent Handover Result . . . 67
14.6.42 E Send End Signal Request . . . 67
14.6.43 E Send End Signal Error . . . 67
14.6.44 E Send End Signal Result . . . 67
14.6.45 E Process Access Signalling Request . . . 68
14.6.46 E Forward Access Signalling Request . . . 68
14.6.47 E Close . . . 68
14.6.48 E Abort . . . 68
14.6.49 E Routing Error . . . 68
14.6.50 ePDG Tunnel Request . . . 69
14.6.51 ePDG Tunnel Error . . . 69
14.6.52 ePDG Tunnel Result . . . 69
14.7 Information Elements . . . 69
14.7.1 Message Type . . . 69
14.7.2 IP Address . . . 72
14.7.3 PDP Info . . . 72
14.7.4 PDP Address . . . 72
14.7.5 PDP Context ID . . . 74
14.7.6 Auth tuple . . . 74
14.7.7 RAND . . . 74

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

14.7.8 SRES . . . 74
14.7.9 Kc . . . 74
14.7.10 IK . . . 74
14.7.11 CK . . . 75
14.7.12 AUTN . . . 75
14.7.13 AUTS . . . 75
14.7.14 RES . . . 75
14.7.15 CN Domain . . . 75
14.7.16 Cancellation Type . . . 75
14.7.17 IE Identifier (informational) . . . 76
14.7.18 Empty field . . . 77
14.7.19 IMSI . . . 77
14.7.20 ISDN-AddressString / MSISDN / Called Party BCD Number . . . 77
14.7.21 Access Point Name . . . 78
14.7.22 Quality of Service Subscribed Service . . . 78
14.7.23 PDP-Charging Characteristics . . . 78
14.7.24 Protocol Configuration Options (PCO) . . . 79
14.7.25 HLR Number encoded as 3GPP TS 09.02 ISDN-AddressString . . . 79
14.7.26 Cause . . . 79
14.7.27 Supplementary Service Info . . . 79
14.7.28 IMEI . . . 79
14.7.29 IMEI Check Result . . . 79
14.7.30 Message Class . . . 80
14.7.31 Source Name . . . 80
14.7.32 Destination Name . . . 80
14.7.33 AN-APDU . . . 80
14.7.34 RR Cause . . . 81
14.7.35 BSSAP Cause . . . 81
14.7.36 Session Management Cause . . . 81
14.8 Session (transaction) management . . . 81
14.8.1 Session ID . . . 81
14.8.2 Session State . . . 81
14.8.3 SM-RP-MR (Message Reference) . . . 82
14.8.4 SM-RP-DA (Destination Address) . . . 82
14.8.5 SM-RP-OA (Originating Address) . . . 82
14.8.6 Coding of SM-RP-DA / SM-RP-OA IEs . . . 82
14.8.7 SM-RP-UI (SM TPDU) . . . 83
14.8.8 SM-RP-Cause (RP Cause value) . . . 83
14.8.9 SM-RP-MMS (More Messages to Send) . . . 83
14.8.10 SM Alert Reason . . . 84

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**15 Counters** **84**

15.1 Rate Counters . . . 84

**16 Osmo Stat Items** **85**

**17 Osmo Counters** **85**

**18 Glossary** **85**

**A Osmocom TCP/UDP Port Numbers** **94**

**B Bibliography / References** **95**

B.0.0.0.1 References . . . 95

**C GNU Free Documentation License** **100**

C.1 PREAMBLE . . . 100

C.2 APPLICABILITY AND DEFINITIONS . . . 100

C.3 VERBATIM COPYING . . . 101

C.4 COPYING IN QUANTITY . . . 101

C.5 MODIFICATIONS . . . 101

C.6 COMBINING DOCUMENTS . . . 103

C.7 COLLECTIONS OF DOCUMENTS . . . 103

C.8 AGGREGATION WITH INDEPENDENT WORKS . . . 103

C.9 TRANSLATION . . . 103

C.10 TERMINATION . . . 103

C.11 FUTURE REVISIONS OF THIS LICENSE . . . 104

C.12 RELICENSING . . . 104

C.13 ADDENDUM: How to use this License for your documents . . . 104

Copyright © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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

### 4.1 About OsmoSGSN

OsmoSGSN is the Osmocom implementation of the GPRS SGSN (Serving Gprs Support Node) element inside the GPRS network. The SGSN plays a similar central function to the GPRS network as the MSC plays in the GSM network.

The SGSN is connected on the downlink side to Gb interfaces of the BSS, specifically the PCU inside the BSS. The SGSN is further connected by the GTP protocol to the GGSN which terminates the tunnels towards the external packet data network (e.g. IPv4).

OsmoSGSN supports both a PCU that is co-located with(in) the BTS, as well as a PCU that is co-located with(in) the BSC. In combination with OsmoNITB/OsmoBSC/OsmoBTS, the PCU is co-located within the BTS.

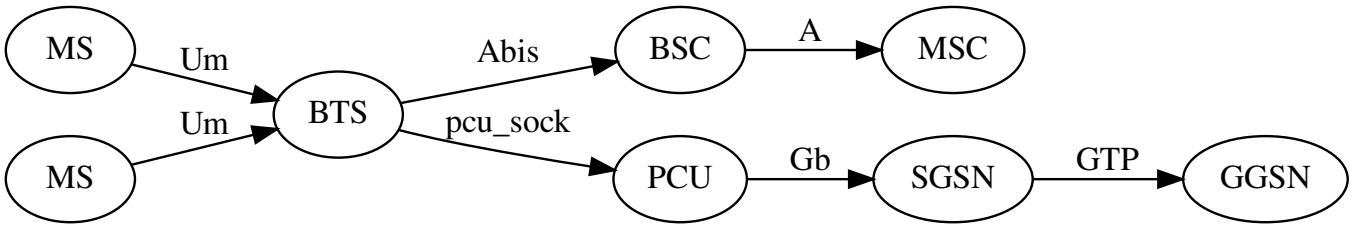



Figure 1: GPRS network architecture with PCU in BTS

### 4.2 Software Components

OsmoSGSN contains a variety of different software components, which we'll quickly describe in this section.

#### 4.2.1 Gb Implementation

OsmoSGSN implements the ETSI/3GPP specified Gb interface, including TS 08.16 (NS), TS 08.18 (BSSGP) and TS 08.64 (LLC) protocols. As transport layers for NS, it supports NS/IP (NS encapsulated in UDP/IP), as well as NS/FR/GRE/IP. The latter is provided in order to use a Router with Ethernet and Frame Relay interface to convert to actual physical Frame Relay medium, which is not directly supported by OsmoSGSN.

The actual Gb Implementation is part of the libosmogb library, which is in turn part of the libosmocore software package. This allows the same Gb implementation to be used from osmo-pcu, osmo-gbproxy as well as OsmoSGSN.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 4.2.2 GTP Implementation

OsmoSGSN uses the libgtp implementation originating from OsmoGGSN. It supports both GTPv0 and GTPv1.

#### 4.2.3 GMM Implementation

The GPRS Mobility Management implementation is quite simplistic at this point. It supports the GPRS ATTACH and GPRS ROUTING AREA UPDATE procedures, as well as GPRS ATTACH and GPRS DETACH.

#### 4.2.4 LLC Implementation

The LLC (Logical Link Control) implementation of OsmoSGSN only supports non-acknowledged mode, as this is the most common use case in real-world GPRS networks.

It does support both TCP/IP header compression according to RFC1144 and payload compression according to V.42bis

The LLC implementation does support LLC encryption with ciphers GEA3 and GEA4. For encryption to work the auth policy needs to be set to remote and the SGSN connected to an HLR containing the subscriber data including key material. Other auth policys will not work with encryption.

#### 4.2.5 Session Management Implementation

The session management procedures ACTIVATE PDP CONTEXT and DEACTIVATE PDP CONTEXT are supported. However, no MODIFY PDP CONTEXT and no Network-initiated PDP context activation is possible. This is again covering the predominant use cases and configurations in GPRS real-world networks while skipping the more esoteric features.

Multiple PDP contexts can be attached by a single MS.

Multiple GGSNs can be configured and routing to a GGSN can be configured based on APN. Dynamic lookup of GGSNs though DNS-based APN resolving is also possible.

### 4.3 Limitations

At the time of writing, OsmoSGSN still has a number of limitations, which are a result of the demand-driven Open Source development model. If you require any of those features, please consider implementing and contributing them, or contracting the existing OsmoSGSN developers for performing that work.

Known Limitations include:

- No paging coordination between SGSN and MSC
- No SMS over Ps support

## 5 Running OsmoSGSN

The OsmoSGSN executable (`osmo-sgsn`) offers the following command-line options:

### 5.1 SYNOPSIS

**osmo-sgsn** [-hl-V] [-d *DBGMASK*] [-D] [-c *CONFIGFILE*] [-s] [-e *LOGLEVEL*]

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 5.2 OPTIONS

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

**-V, --version**
Print the compile-time version number of the OsmoSGSN program

**-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 8 for further information.

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

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

**-s, --disable-color**
Disable colors for logging to stderr. This has mostly been deprecated by VTY based logging configuration, see Section 8 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 8 for more information.

## 6 Control interface

The actual protocol is described in Section 12, the variables common to all programs using it are described in Section 12.2. Here we describe variables specific to OsmoSGSN.

Table 2: Variables available over control interface

| Name | Access | Trap | Value | Comment |
|---|---|---|---|---|
| subscriber-list-active-v1 | RO | No | "<imsi>,<addr>" | See Section 6.1 for details. |

### 6.1 subscriber-list-active-v1

Return the list of active subscribers as a concatenated set of pairs "<imsi>", "addr" where first element of the pair is subscriber's IMSI and the second element (which might be empty) is the subscriber's address. The address value might be "none", "invalid" and "PPP" in addition to actual IP address. In case of IP address it will be prefixed with "IPv4" or "IPv6" string depending on the version of IP protocol.

## 7 The Osmocom VTY Interface

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

Copyright © 2013-2024 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 3: 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

## 7.1 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.

## 7.2 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.

## 7.3 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 7.3.1 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 7.3.2 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.

### 7.3.3 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 © 2013-2024 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 © 2013-2024 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
```

### 7.3.4 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 © 2013-2024 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.

### 7.3.5 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 © 2013-2024 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.

# 8 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.

## 8.1 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 ?`

## 8.2 Log levels

For each of the log categories (see Section 8.1), 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 © 2013-2024 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.

## 8.3 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.

## 8.4 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

## 8.5 Log targets

Each of the log targets represent certain destination for log messages. It can be configured independently by selecting levels (see Section 8.2) for categories (see Section 8.1) as well as filtering (see Section 8.4) and other options like `logging timestamp` for example.

### 8.5.1 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 8.1 for more details on categories and Section 8.2 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 8.4.

**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`

### 8.5.2 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.

### 8.5.3 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 © 2013-2024 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.

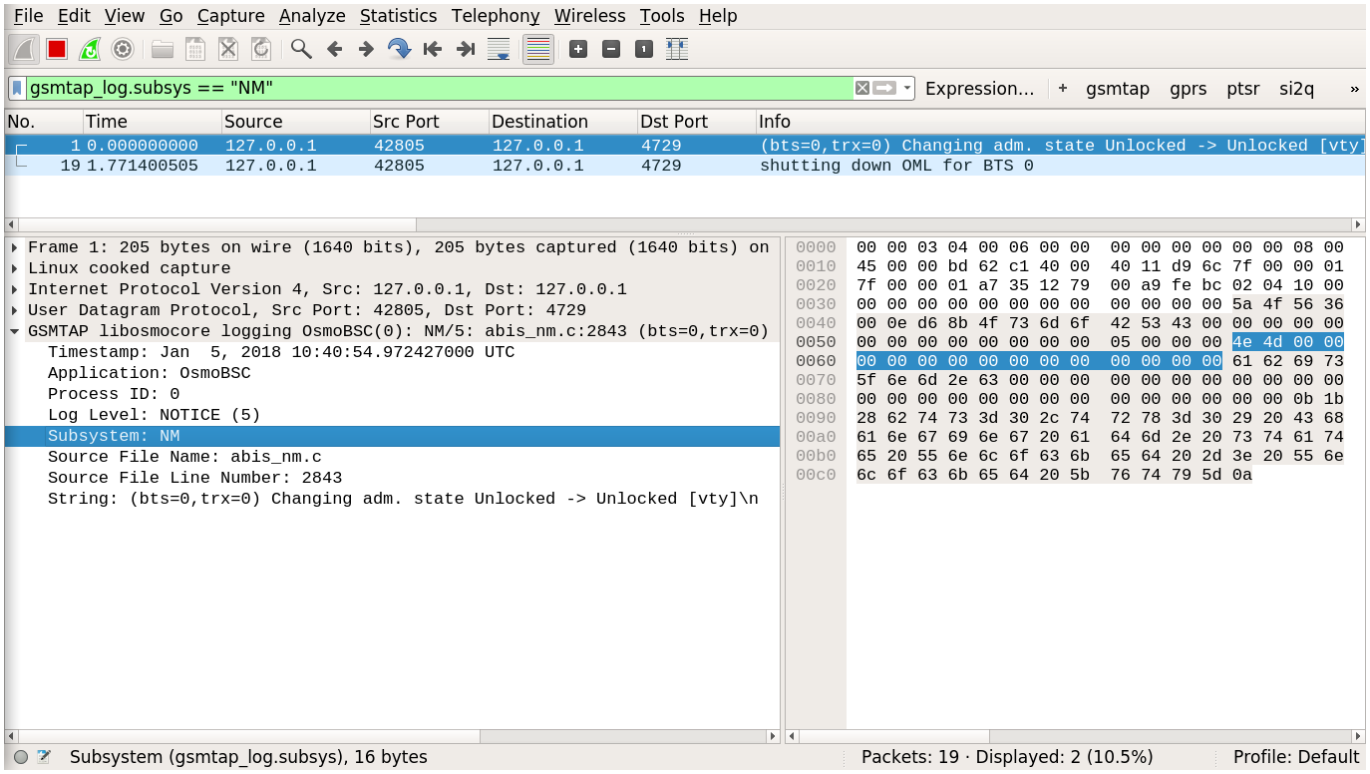



Figure 2: Wireshark with logs delivered over GSMTAP

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 © 2013-2024 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.

### 8.5.4 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.

### 8.5.5 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 8.5.6 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 © 2013-2024 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*.

#### 8.5.7 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)#
```

# 9 Configuring OsmoSGSN

Contrary to other network elements (like OsmoBSC, OsmoNITB), the OsmoSGSN has a relatively simple configuration.

On the one hand, this is primary because the PCU configuration happens from the BSC side.

On the other hand, it is because the Gb interface does not need an explicit configuration of each PCU connecting to the SGSN. The administrator only has to ensure that the NS and BSSGP layer identities (NSEI, NSVCI, BVCI) are unique for each PCU connecting to the SGSN.

## 9.1 Configuring the Gp interface (towards GGSN)

The Gp interface is the GTP-C and GTP-U based interface between the SGSN and the GGSNs. It is implemented via UDP on well-known source and destination ports.

When an MS requests establishment of a PDP context, it specifies the APN (Access Point Name) to which the context shall be established. This APN determines which GGSN shall be used, and that in turn determines which external IP network the MS will be connected to.

There are two modes in which GGSNs can be configured:

1. static GGSN/APN configuration
2. dynamic GGSN/APN configuration

### 9.1.1 Static GGSN/APN configuration

In this mode, there is a static list of GGSNs and APNs configured in OsmoSGSN via the VTY / config file.

This is a non-standard method outside of the 3GPP specifications for the SGSN, and is typically only used in private/small GPRS networks without any access to a GRX.

**Example: Static GGSN/APN configuration (single catch-all GGSN)**

```
OsmoSGSN(config-sgsn)# gtp local-ip 172.0.0.1 ❶
OsmoSGSN(config-sgsn)# ggsn 0 remote-ip 127.0.0.2 ❷
OsmoSGSN(config-sgsn)# ggsn 0 gtp-version 1 ❸
OsmoSGSN(config-sgsn)# apn * ggsn 0 ❹
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

❶ Configure the local IP address at the SGSN used for Gp/GTP

❷ Specify the remote IP address of the GGSN (for GGSN 0)

❸ Specify the GTP protocol version used for GGSN 0

❹ Route all APN names to GGSN 0

#### 9.1.2 Dynamic GGSN/APN configuration

In this mode, the SGSN will use a DNS-based method to perform the lookup from the APN (as specified by the MS) towards the GGSN IP address.

This is the official method as per the 3GPP specifications for the SGSN, and what is used on GRX.

**Example: Dynamic GGSN/APN configuration**

```
OsmoSGSN(config-sgsn)# gtp local-ip 192.168.0.11 ❶
OsmoSGSN(config-sgsn)# ggsn dynamic ❷
OsmoSGSN(config-sgsn)# grx-dns-add 1.2.3.4 ❸
```

❶ Configure the local IP address at the SGSN used for Gp/GTP

❷ Enable the dynamic GGSN resolving mode

❸ Specify the IP address of a DNS server for APN resolution

### 9.2 Configuring the Gp interface (towards MME)

The Gp interface also contains the GTP-C v1 based interface between the SGSN and the MMEs. This interface between SGSN and MMEs is used to transfer *RAN Information Relay* GTP-C messages between them, which are used as containers to allow PCUs under the SGSN and eNodeBs under MMEs to exchange cell information (RIM).

In the SGSN, this interface re-uses the same socket local configuration as per the GGSN connections (see *gtp local-ip* VTY command in Section 9.1).

Similarly as with GGSNs, (again see Section 9.1), selection of destination peers for the *RAN Information Relay* message can be configured statically or dynamically over GRX.

#### 9.2.1 Static MME/TAI configuration

In this mode, there is a static list of MMEs and TAIs configured in OsmoSGSN via the VTY / config file. One MME in the list can be configured as the *default route*, where all unspecified TAIs are routed too.

This is a non-standard method outside of the 3GPP specifications for the SGSN, and is typically only used in private/small GPRS networks without any access to a GRX.

**Example: Static MME/TAI configuration (single catch-all GGSN)**

```
sgsn
...
 gtp local-ip 192.168.0.10 ❶
 mme test-mme0 ❷
  gtp remote-ip 192.168.0.20 ❸
  gtp ran-info-relay 262 42 3 ❹
  gtp ran-info-relay 262 42 4
 mme test-mme1 ❺
  gtp remote-ip 192.168.0.30
  gtp ran-info-relay default  ❻
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

❶ Configure the local IP address at the SGSN used for Gp/GTP

❷ Configure an MME named "test-mme0"

❸ Specify the remote IP address of the MME (for MME "test-mme0")

❹ Route specified TAIs towards this MME

❺ Configure an MME named "test-mme1"

❻ Route all TAIs with an unspecified MME towards MM "test-mme1"

#### 9.2.2 Dynamic MME/TAI configuration

Dynamic MME/TAI peer look up over GRX is not yet supported by OsmoSGSN.

### 9.3 Authorization Policy

The authorization policy controls by which rules a subscriber is accepted or rejected. The possible options range from accepting just all subscribers without further checking, to a fine grained access-control, handled by an external HLR.

**accept-all**
: All subscribers that attempt to attach to the GPRS network are accepted without further checking. This option is intended to be used for testing in a controlled environment only. A wide-open network may attract subscribers from foreign networks and disrupt their service. It is highly recommended to pick one of the options below.

**remote**
: This option allows to connect OsmoSGSN to an external HLR via the GSUP protocol. This will be the preferred option in larger networks.

**acl-only**
: If no external HLR is available, the network operator has the option to control the access using an access control list. The access control list contains the IMSI numbers of the allowed subscribers. This method offers fine grained access control and is ideal for small networks and lab test environments.

**closed**
: This policy mode softens the strict **acl-only** only mode by also implicitly accepting home network subscribers. The decision is made by the MCC and MNC part of the IMSI number. The combination of MCC and MNC fully identifies a subscribers home network, also known as a Home Network Identity (HNI, i.e. MCC and MNC found at the start of the IMSI, e.g. MCC 901 and MNC 700 with IMSI 901700000003080).

---

**Note**
The policy mode **closed** must not be confused with the equally named policy that is defined for osmo-nitb!

---

**Example: Assign or change authorization policy**

```
OsmoSGSN> enable
OsmoSGSN# configure terminal
OsmoSGSN(config)# sgsn
OsmoSGSN(config-sgsn)# auth-policy acl-only ❶
OsmoSGSN(config-sgsn)# write ❷
Configuration saved to sgsn.cfg
OsmoSGSN(config-sgsn)# end
OsmoSGSN# disable
OsmoSGSN>
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

1. *acl-only* is selected as authorization policy
2. Saves current changes to cofiguration to make this policy persistent

**Example: Access control list**

```
sgsn
 auth-policy acl-only (1)
 imsi-acl add 001010000000003
 imsi-acl add 001010000000002
 imsi-acl add 001010000000001
 imsi-acl add 901700000000068 (2)
```

1. Set the authorization policy
2. Add as many subscribers as required

## 9.4 Subscriber Configuration

As opposed to OsmoNITB, OsmoSGSN does not feature a built-in HLR.

It can thus operate only in the following two modes:

1. Accessing an external HLR (or HLR gateway) via the GSUP protocol
2. Accepting subscribers based on internal ACL (access control list), see also Section 9.3

### 9.4.1 Accessing an external HLR via GSUP

The non-standard GSUP protocol was created to provide OsmoSGSN with access to an external HLR while avoiding the complexities of the TCAP/MAP protocol stack commonly used by HLRs.

A custom HLR could either directly implement GSUP, or an external gateway can be used to convert GSUP to the respective MAP operations.

The primitives/operations of GSUP are modelled to have a 1:1 correspondence to their MAP counterparts. However, the encoding is much simplified by use of a binary TLV encoding similar to Layer 3 of GSM/GPRS.

GSUP performs a challenge-response authentication protocol called OAP, which uses the standard MILENAGE algorithm for mutual authentication between OsmoSGSN and the HLR/HLR-GW.

**Example: Using an external HLR via GSUP**

```
OsmoSGSN(config-sgsn)# gsup remote-ip 2.3.4.5 (1)
OsmoSGSN(config-sgsn)# gsup remote-port 10000 (2)
OsmoSGSN(config-sgsn)# gsup oap-k 000102030405060708090a0b0c0d0e0f (3)
OsmoSGSN(config-sgsn)# gsup oap-opc 101112131415161718191a1b1c1d1e1f (4)
```

1. Configure the IP address of the (remote) HLR or HLR-GW
2. Configure the TCP port of the (remote) HLR or HLR-GW
3. Specify the OAP shared key
4. Specify the OAP shared OPC

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

## 9.5 CDR configuration

OsmoSGSN can write a text log file containing CDR (call data records), which are commonly used for accounting/billing purpose.

**Example: CDR log file configuration**

```
OsmoSGSN(config-sgsn)# cdr filename /var/log/osmosgsn.cdr
OsmoSGSN(config-sgsn)# cdr interval 600 ❶
```

❶ Periodically log existing PDP contexts every 600 seconds (10 min)

The CDR file is a simple CSV file including a header line naming the individual fields of each CSV line.

### 9.5.1 CDR CTRL interface

Independently of whether logging CDR to a file is enabled or not, OsmoSGSN can also provide delivery of CDR through the CTRL interface. CDR are sent by means of TRAP messages with variable name *cdr-v1*, and its value is filled using the same CSV line format as in the log file, but without CSV header line.

**Example: CDR delivery through CTRL TRAP messages**

```
OsmoSGSN(config-sgsn)# cdr trap
```

### 9.5.2 CDR Format

Table 4: Description of CSV fields in OsmoSGSN CDR file

| Field Name | Description |
|---|---|
| timestamp | Timestamp in YYYYMMDDhhmmssXXX where XXX are milli-seconds |
| imsi | IMSI causing this CDR |
| imei | IMEI causing this CDR |
| msisdn | MSISDN causing this CDR (if known) |
| cell_id | Cell ID in which the MS was registered last |
| lac | Location Area Code in which the MS was registered last |
| hlr | HLR of the subscriber |
| event | Possible events are explained below in Table 6 |

If the *event* field describes a pdp context related action (starts with *pdp-*), then the following extra CSV fields are appended to the line:

Table 5: Description of extra CSV fields for pdp context related events

| Field Name | Description |
|---|---|
| pdp_duration | duration of the PDP context so far |
| ggsn_addr | GGSN related to the PDP context |
| sgsn_addr | SGSN related to the PDP context |
| apni | APN identifier of the PDP context |
| eua_addr | IP address allocated to the PDP context |
| vol_in | Number of bytes in MO direction |
| vol_out | Number of bytes in MT direction |
| charging_id | Related charging ID |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

Table 6: Description of OsmoSGSN CDR Events

| Event | Description |
|---|---|
| attach | GMM ATTACH COMPLETE about to be sent to MS |
| update | GMM ROUTING AREA UPDATE COMPLETE about to be sent to MS |
| detach | GMM DETACH REQUEST received from MS |
| free | Release of the MM context memory |
| pdp-act | GTP CREATE PDP CONTEXT CONFIRM received from GGSN |
| pdp-deact | GTP DELETE PDP CONTEXT CONFIRM received from GGSN |
| pdp-terminate | Forced PDP context termination during MM context release |
| pdp-free | Release of the PDP context memory |
| pdp-periodic | Triggered by periodic timer, see VTY cmd *cdr interval* |

## 9.6 User traffic compression

In order to save GPRS bandwith, OsmoSGSN implements header and data compression schemes which will reduce the packet length.

### 9.6.1 Header compression

On TCP/IP connections, each packet is prepended with a fairly long TCP/IP header. The header contains a lot of static information that never changes throughout the connection. (source and destination address, port numbers etc.) OsmoSGSN implements a TCP/IP header compression scheme called RFC1144, also known as SLHC. This type of header compression removes the TCP/IP header entirely and replaces it with a shorter version, that only contains the information that is absolutely necessary to identify and check the packet. The receiving part then restores the original header and forwards it to higher layers.

**compression rfc1144 passive**
: TCP/IP header compression has to be actively requested by the modem. The network will not promote compression by itself. This is the recommended mode of operation.

**compression rfc1144 active slots <1-256>**
: TCP/IP header compression is actively promoted by the network. Modems may still actively request different compression parameters or reject the offered compression parameters entirely. The number of slots is the maximum number of packet headers per subscriber that can be stored in the codebook.

**Example: Accept compression if requested**

```
sgsn
 compression rfc1144 passive
```

**Example: Actively promote compression**

```
sgsn
 compression rfc1144 active slots 8
```

**Example: Turn off compression**

```
sgsn
 no compression rfc1144
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**Note**
The usage of TCP/IP options may disturb the RFC1144 header compression scheme. TCP/IP options may render RFC1144 ineffective if variable data is encoded into the option section of the TCP/IP packet. (e.g. TCP option 8, Timestamp)

### 9.6.2 Data compression

Data compression works on the raw packet data, including the header part of the packet. If enabled, header compression is applied first before data compression is applied. OsmoSGSN implements the V.42bis data compression scheme.

**compression v42bis passive**
V42bis data compression has to be actively requested by the modem. The network will not promote compression by itself. This is the recommended mode of operation.

**compression v42bis active direction (ms|sgsn|both) codewords <512-65535> strlen <6-250>**
V42bis data compression is actively promoted by the network. Modems may still actively request different compression parameters or reject the offered compression parameters entirely. The direction configures which sides are allowed to send compressed packets. For most cases, compressing *both* directions will be the preferred option. The following to parameters configure the codebook size by the maxium number (*codewords*) and size (*strlen*) of entries.

**Example: Accept compression if requested**

```
sgsn
 compression v42bis passive
```

**Example: Actively promote compression**

```
sgsn
 compression v42bis active direction both codewords 512 strlen 20
```

**Example: Turn off compression**

```
sgsn
 no compression v42bis
```

## 9.7 Encryption

Encryption can be enabled if the auth-policy is set to remote and the HLR subscriber entries contain the keys of the SIM card. See Example: Using an external HLR via GSUP on how to connect to an external HLR.

**Example: Turn on encryption (GEA3 and GEA4)**

```
sgsn
 encryption gea 3 4
```

**Example: Turn off encryption (GEA0)**

```
sgsn
 encryption gea 0
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 9.8 Configure SCCP/M3UA to accept *IuPS* links

OsmoSGSN acts as client to contact an STP instance and establish an SCCP/M3UA link.

An example configuration of OsmoSGSN's SCCP link:

```
cs7 instance 0
 point-code 0.23.4
 asp asp-clnt-OsmoSGSN 2905 0 m3ua
  remote-ip 127.0.0.1
  role asp
  sctp-role client
 as as-clnt-OsmoSGSN m3ua
  asp asp-clnt-OsmoSGSN
  routing-key 0 0.23.4
```

This configuration is explained in detail in Section 10.

## 10 Configure SCCP/M3UA

All CNI programs using SCCP/M3UA act as M3UA ASP role and SCTP client, expecting to connect to a Signalling Gateway (STP/SG) implementing the M3UA SG role as SCTP server. The STP/SG then routes M3UA messages between its ASPs, typically by point-codes.

For an introduction about SCCP/M3UA/SS7/SIGTRAN technology, please see the chapter *Signaling Networks: SS7 and SIGTRAN* in the OsmoSTP user manual.

In an all-Osmocom CNI, the typical simple/minimal usage is:

- OsmoSTP acts as the STP/SG (server role) and routes between the ASP,
- All other Osmocom CNI programs act as SCTP client and provide ASP implementations.

For example, in an all-Osmocom minimal setup,

- OsmoMSC contacts an OsmoSTP and subscribes its point-code 0.23.1;
- then OsmoBSC also contacts the same OsmoSTP, subscribes with its own point-code 1.23.3.
- Using these established links, OsmoBSC initiates an A-interface link by directing a BSSAP RESET message to the MSC's point-code 0.23.1,
- and the RESET ACK response from the MSC is routed back to the BSC's point-code 1.23.3.

The details of SCCP/M3UA are configured in the *cs7* section of the VTY configuration.

Osmocom programs automatically configure missing SCCP/M3UA configuration, by assuming sane defaults for small/minimal all-Osmocom installations, which may not be what you want in larger networks integrating with non-Osmocom core network elements.

If no explicit `routing-key` is set, it may be determined at runtime by negotiation with OsmoSTP — see OsmoSTP manual chapter "Osmocom M3UA Routing Key Management Extensions", regarding config option `accept-asp-connections dynamic-permitted`.

The complete active configuration of an Osmocom program can be obtained by the VTY command `show cs7 config` (the usual `show running-config` omits automatically configured items). Here is an example of OsmoMSC's default configuration:

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

```
OsmoMSC> show cs7 config
cs7 instance 0
 point-code 0.23.1
 asp asp-clnt-OsmoMSC-A-Iu 2905 0 m3ua
  remote-ip 127.0.0.1
  role asp
  sctp-role client
 as as-clnt-OsmoMSC-A-Iu m3ua
  asp asp-clnt-OsmoMSC-A-Iu
  routing-key 2 0.23.1
```

At the time of writing, SCCP/M3UA links involving Osmocom program are:

- A-interface: OsmoBSC to OsmoMSC
- IuCS-interface: OsmoHNBGW to OsmoMSC
- IuPS-interface: OsmoHNBGW to OsmoSGSN
- Lb-interface: OsmoSMLC to OsmoBSC

On the SCTP/IP level, those connections are actually all established from the respective program (BSC, MSC, HNBGW, SGSN, SMLC) to OsmoSTP. Hence, if you look at the traffic in a protocol analyzer like wireshark, at IP level, you will see each of those programs establishing an SCTP association from a random local IP to the well-known SCTP port for M3UA (2905) at the OsmoSTP.

Those star-connections for M3UA/SCTP then are the transport network for higher level protocols like SCCP. OsmoSTP then acts as central router for SCCP-level message exchange between all the connected programs.

## 10.1 Connect to STP Instance

Establishing an SCCP/M3UA link towards a remote STP instance can be configured as:

```
cs7 instance 0
 asp my-asp 2905 0 m3ua
  # IP address of the remote STP:
  remote-ip 10.23.24.1
  # optional: local bind to a specific IP
  local-ip 10.9.8.7
  role asp
  sctp-role client
```

Be aware that such an `asp` needs to be linked to an `as`, see Section 10.5.

By default, an STP instance is assumed to listen on the default M3UA port (2905) on the local host. That means in general `127.0.0.1` will be used as default remote SCTP address, and `::1` will be added to the SCTP association if IPv6 support is available on the system.

**Note**
OsmoSTP listens by default on `::` if IPv6 is enabled on the system, and on `0.0.0.0` otherwise. Address `::` actually superseeds `0.0.0.0`, meaning it will listen on all IPv4 and IPv6 addresses available on the system.



**Caution**
Some applications overwrite the default target remote address to be `localhost`. If IPv6 support is available on the system, `localhost` will usually resolve to `::1`, otherwise it will usually resolve to `127.0.0.1`.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

## 10.2 Local Point-Code

Each CNI program on an SCCP/M3UA link typically has a local point-code, configurable by:

```
cs7 instance 0
 point-code 7.65.4
```

If an explicit routing context is configured, this point-code is repeated in the `routing-key` configuration:

```
cs7 instance 0
 point-code 0.23.1
 as my-as m3ua
  routing-key 2 0.23.1
```

See also Section 10.4.

## 10.3 Remote Point-Code

Programs establishing communication across SCCP links need a remote SCCP address, typically by point-code, to contact.

For example,

- OsmoBSC needs to know the MSC's point-code, to be able to establish the A-interface.
- OsmoHNBGW needs to know the MSC's point-code, to be able to establish the IuCS-interface.
- OsmoHNBGW needs to know the SGSN's point-code, to be able to establish the IuPS-interface.

To maintain remote SCCP addresses, each `cs7` instance maintains an SCCP address book:

```
cs7 instance 0
 sccp-address remote-pc-example
  point-code 1.23.1
```

This address book entry on its own has no effect. It is typically referenced by specific configuration items depending on the individual programs.

Examples:

- An OsmoBSC configures the MSC's remote SCCP address:

```
cs7 instance 0
 sccp-address my-remote-msc
  point-code 1.23.1
msc 0
 msc-addr my-remote-msc
```

- An HNBGW configures both the remote MSC's and SGSN's SCCP addresses:

```
cs7 instance 0
 sccp-address my-msc
  point-code 0.23.1
 sccp-address my-sgsn
  point-code 0.23.2
hnbgw
 iucs
  remote-addr my-msc
 iups
  remote-addr my-sgsn
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

Besides a point-code, an SCCP address can have several routing indicators:

- PC: routing by point-code is the default for Osmocom.
- GT: routing by Global Title is configurable by `routing-indicator GT`.
- IP: routing by IP address is configurable by `routing-indicator IP`.

In OsmoSTP, only routing by point-code is currently implemented.

## 10.4 Point-Code Format

Point-codes can be represented in various formats. For details, see OsmoSTP manual, chapter "Point Codes".

By default, Osmocom uses a point-code representation of 3.8.3, i.e. first digit of 3 bit, second digit of 8 bit, and third digit of 3 bit.

```
cs7 instance 0
 point-code format 3 8 3
 point-code 0.23.1
```

Often, point-codes are also represented as a single decimal number:

```
cs7 instance 0
 point-code format 24
 point-code 185
```

It is also possible to use a dash as delimiter.

```
cs7 instance 0
 point-code delimiter dash
 point-code 0-23-1
```

## 10.5 AS and ASP

Each CNI program needs at least one Application Server `as` and one Application Server Process `asp` configured on its `cs7` to be able to communicate on SCCP/M3UA. An `asp` needs to be part of at least one `as`. For details, see the OsmoSTP manual, chapters "Application Server" and "Application Server Process".

In Osmocom's `cs7`, any amount of `as` and `asp` can be configured by name, and an `as` references the `asp` entries belonging to it by their names.

In a simple/minimal Osmocom setup, an Osmocom CNI program would have exactly one `as` with one `asp`.

For example:

```
cs7 instance 0
 asp my-asp 2905 0 m3ua
  # where to reach the STP:
  remote-ip 127.0.0.1
  role asp
  sctp-role client
 as my-as m3ua
  asp my-asp
```

In Osmocom CNI programs, it is possible to omit the `as` and/or `asp` entries, which the program will then attempt to configure automatically.

When configuring both `as` and `asp` manually, make sure to link them by name. For example, the following configuration will **fail**, because `as` and `asp` are not linked:

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

```
cs7 instance 0
 asp my-asp 2905 0 m3ua
  remote-ip 127.0.0.1
  role asp
  sctp-role client
 as my-as m3ua
  routing-key 2 0.23.1
```

To **fix** above config, link the `asp` to an `as` by adding `asp my-asp`:

```
cs7 instance 0
 asp my-asp 2905 0 m3ua
  remote-ip 127.0.0.1
  role asp
  sctp-role client
 as my-as m3ua
  asp my-asp
  routing-key 2 0.23.1
```

## 10.6 Subsystem Number (SSN)

Osmocom CNI programs typically route SCCP/M3UA messages by PC+SSN: each ASP, having a given SCCP address, receives messages for one or more specific subsystems, identified by a Subsystem Number (SSN).

For example, the A-interface between BSC and MSC uses SSN = BSSAP (254). In Osmocom programs, SSNs do not need to be configured; they implicitly, naturally relate to the interfaces that a program implements.

For example, OsmoBSC takes the configured remote MSC's SCCP address and adds the SSN = BSSAP to it in order to contact the MSC's A-interface. To receive A-interface messages from the MSC, OsmoBSC subscribes a local user for this SSN on the ASP.

## 10.7 Routing Context / Routing Key

In SCCP/M3UA, messages can be routed by various Routing Indicators (PC+SSN, PC, GT, ...). Osmocom CNI programs typically use PC+SSN as Routing Indicator.

On the SG (for example OsmoSTP), each ASP's distinct Routing Indicator needs to be indexed by a distinct Routing Context (a simple index number scoped per SG), to forward M3UA to the correct peer.

The Osmocom SG implementation employs Routing Key Management (RKM, see OsmoSTP manual) to automatically determine a distinct Routing Context index for each connected ASP. Routing Contexts can also be configured manually — some non-Osmocom SG implementations require this.

Each Routing Context is associated with a Routing Indicator and address; this association is called a Routing Key.

For example, to configure an OsmoBSC with a local point-code of 1.23.3 to receive M3UA with Routing Context of 2 and RI=PC:

```
cs7 instance 0
 point-code 1.23.3
 as my-as m3ua
  routing-key 2 1.23.3
```

Osmocom programs so far implement Routing Keys by Destination Point Code (DPC), plus optional Subsystem Number (SSN) and/or Service Indicator (SI):

```
routing-key RCONTEXT DPC
routing-key RCONTEXT DPC si (aal2|bicc|b-isup|h248|isup|sat-isup|sccp|tup)
routing-key RCONTEXT DPC ssn SSN
routing-key RCONTEXT DPC si (aal2|bicc|b-isup|h248|isup|sat-isup|sccp|tup) ssn SSN
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 10.7.1 M3UA without Routing Context IE / Routing Context *0*

As per the M3UA specification, the use of the routing context IE is optional as long as there is only one AS within an ASP. As soon as there are multiple different AS within one ASP, the routing context IE is mandatory, as it is the only clue to differentiate which of the ASs a given message belongs to.

In the Osmocom M3UA implementation, it is generally assumed that a routing context IE is always used, for the sake of clarity.

However, the routing context ID of *0* has the special meaning of *do not encode a routing context IE on transmit*.

So if you configure an application like OsmoBSC to use routing context 0, then no routing context IE will be included in outbound M3UA messages.

This special interpretation of *0* within the Osmocom M3UA implementation however means that we can not represent M3UA with a routing context IE that actually contains *0* as a numeric identifier.

So you only have the following options: * Using M3UA with routing context (1..N) * Using M3UA without routing context (0)

#### 10.7.2 Example: Static Routing

Osmocom SS7 supports dynamic routing key registration via M3UA Routing Key Management (RKM), allowing minimal SS7 configuration. If all of your components support dynamic RKM, you should probably use it: see `accept-asp-connections dynamic-permitted` in osmo-stp.cfg.

This chapter explains how to configure osmo-stp if dynamic RKM is not an option.

In this example, let's connect osmo-bsc via osmo-stp to osmo-msc using only static SS7 routing.

```
BSC        <--RK-1-->  STP         <--RK-3--> MSC
IP 1.1.1.1             IP 2.2.2.2             IP 3.3.3.3
M3UA 2905              M3UA 2905              M3UA 2905
PC 1.1.1                                      PC 3.3.3
```

Every one static route fanning out from STP gets assigned a distinct Routing Key — a simple integer number. Above, the BSC's link has RK 1, the MSC's link has RK 3.

For static routing, the M3UA port numbers must be fixed, i.e. there must be no `0` for a client's local port as in `asp foo 2905 0 m3ua`. Instead, you may use `asp foo 2905 2905 m3ua`.

The BSC needs to configure:

- its own point-code — has to match the PC configured for the BSC in osmo-stp.cfg
- the routing key — has to match the RK assigned to BSC's PC in osmo-stp.cfg
- the MSC's point-code — has to match the PC in osmo-stp.cfg and osmo-msc.cfg
- local and remote IP:ports for M3UA — have to match the IP:ports in osmo-stp.cfg

The MSC needs to configure:

- its own point-code — has to match the PC configured for the MSC in osmo-stp.cfg
- the routing key — has to match the RK assigned to MSC's PC in osmo-stp.cfg
- local and remote IP:ports for M3UA — have to match the IP:ports in osmo-stp.cfg

The STP needs to configure:

- all point-codes — they have to match the PCs in osmo-bsc.cfg and osmo-msc.cfg
- all routing keys — they have to match the RKs used in osmo-bsc.cfg and osmo-msc.cfg

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

- local and remote IP:ports for M3UA — have to match the IP:ports in osmo-bsc.cfg and osmo-msc.cfg

**osmo-bsc.cfg**

```
cs7 instance 0
 point-code 1.1.1

 asp mybsc-0 2905 2905 m3ua
  remote-ip 2.2.2.2
  local-ip 1.1.1.1
  sctp-role client
 as mybsc0 m3ua
  asp mybsc0-0
  routing-key 1 1.1.1

 sccp-address mymsc
  routing-indicator PC
  point-code 3.3.3

msc 0
 msc-addr mymsc
```

**osmo-stp.cfg**

```
cs7 instance 0
 xua rkm routing-key-allocation static-only
 listen m3ua 2905
  accept-asp-connections pre-configured
  local-ip 2.2.2.2

 # asp <name> <remote-port> <local-port|0> m3ua
 asp mybsc-0 2905 2905 m3ua
  remote-ip 1.1.1.1
  local-ip 2.2.2.2
 as mybsc m3ua
  asp bsc-0
  routing-key 1 1.1.1

 asp mymsc-0 2905 2905 m3ua
  remote-ip 3.3.3.3
  local-ip 2.2.2.2
 as mymsc m3ua
  asp mymsc-0
  routing-key 3 3.3.3

 route-table system
  update route 1.1.1 7.255.7 linkset mybsc
  update route 3.3.3 7.255.7 linkset mymsc
```

**osmo-msc.cfg**

```
cs7 instance 0
 point-code 3.3.3

 asp mymsc-0 2905 2905 m3ua
  remote-ip 2.2.2.2
  local-ip 3.3.3.3
  sctp-role client
 as mymsc0 m3ua
  asp mymsc0-0
  routing-key 3 3.3.3
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

For comparison, the same setup with dynamic routing key management is a lot shorter, especially at osmo-stp.cfg, and there is no need to manually configure point-codes and routing keys between STP and {BSC,MSC}:

**osmo-bsc.cfg**

```
cs7 instance 0
 point-code 1.1.1

 asp mybsc-0 2905 0 m3ua
  remote-ip 2.2.2.2
  local-ip 1.1.1.1
  sctp-role client
 as mybsc0 m3ua
  asp mybsc0-0

 sccp-address mymsc
  routing-indicator PC
  point-code 3.3.3

msc 0
 msc-addr mymsc
```

**osmo-stp.cfg**

```
cs7 instance 0
 xua rkm routing-key-allocation dynamic-permitted
 listen m3ua 2905
  accept-asp-connections dynamic-permitted
  local-ip 2.2.2.2
```

**osmo-msc.cfg**

```
cs7 instance 0
 point-code 3.3.3

 asp mymsc-0 2905 0 m3ua
  remote-ip 2.2.2.2
  local-ip 3.3.3.3
  sctp-role client
 as mymsc0 m3ua
  asp mymsc0-0
```

# 11 Gb/NS Network Service

*libosmogb* is part of the libosmocore.git repository and implements the Gb interface protocol stack consisting of the NS and BSSGP layers. It is used in a variety of Osmocom projects, including OsmoSGSN, OsmoPCU and OsmoGbProxy.

**Note**
[3gpp-ts-48-016] specifies Network Service

## 11.1 Gb interface variants

There are multiple variants of the Gb interface. This section tries to provide an overview into what those variants are, how they differ from each other.

The two peers involved in any Gb interface must always be in agreement about the specific Gb interface variant before they are able to connect.

The following variants are supported by Osmocom:

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

- Gb-over-Frame-Relay over E1/T1
- Gb-over-IP "ip.access style"
- Gb-over IP 3GPP static configuration
- Gb-over-IP 3GPP auto-configuration

### 11.1.1 Gb over Frame Relay over E1/T1

Historically, this is the first Gb interface that was specified as part of GSM Release 97 when GPRS was first introduced.

Like all other terrestrial GSM interfaces, it uses circuit-switched technology from the PDH/ISDN family of systems: E1 or T1 lines as per ITU-T G.703 / G.704.

GSM TS 08.16 and later [3gpp-ts-48-016] specify that Frame Relay (FR) shall be used as transport layer between the E1/T1 bit-stream and the NS-level Gb messages.

Two peer entities such as a GPRS BSS and a SGSN are interconnected by a NS-VCG (Virtual Connection Group) consisting of any number of NS-VCs (Virtual Connections).

Each NS-VC in turn operates over a Frame Relay Permanent Virtual Circuit (PVC), identified by its DLCI (Data Link Connection Identifier).

The protocol stacking is BSSGP/NS/FR/E1.

#### 11.1.1.1 FR Driver Support

The Osmocom NS/FR implementation currently requires the individual Frame Relay Links to be exposed as Linux kernel HDLC net-devices. The Osmocom NS implementation has to be instructed which `hdlcX` network devices it shall use for each NS-VC, and which DLCIs to use on them.

The Linux kernel Frame Relay LMI support (which only implements the user role anyway) is not used. Instead, the ITU-T Q.933 LMI is implemented as part of the Osmocom NS code in libosmogb. Osmocom NS code configures the `hdlcX` device to match the correct mode (fr) and lmi (none). This is equivalent to the user-space command `sethdlc hdlcX fr lmi none`. The net-devices will be also brought *up* by the Osmocom NS code equivalent to `ip link set hdlcX up` command.

As the Osmocom Gb implementation uses AF_PACKET sockets on those `hdlcX` network interfaces, the respective program must be running with `CAP_NET_RAW` capability.

### 11.1.2 Gb over Frame Relay encapsulated in GRE/IP

This is a variant of the Gb-over-FR specified above. However, an external router (e.g. certain ancient Cisco routers) is used to take the Frame Relay frames from the physical E1/T1 TDM circuit and wrap them into the GRE encapsulation as per IETF RFC 2784.

**Note**
GRE/IP has been removed from Osmocom NS code.

### 11.1.3 Gb over IP "ip.access style"

This is a non-standard variant of Gb which is not found in the GSM/3GPP specifications.

It uses an UDP/IP based transport layer, while not yet implementing the IP-SNS that is normally required by a true 3GPP Gb over IP interface described further below. Hence, this variant resembles an intermediate state where a Gb interface originally designed for Frame Relay is used over IP without any of the IP-specific procedures specified by 3GPP.

The major difference to 3GPP Gb over IP specified below are:

- No support for the IP-SNS and its SNS-SIZE, SNS-ADD, SNS-DELETE, SNS-WEIGHT procedures.
- Use of the NS-RESET, NS-BLOCK and NS-UNBLOCK procedures which are normally forbidden over an IP network.

The protocol stacking is BSSGP/NS/UDP/IP.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 11.1.4 Gb over IP 3GPP static and auto-configuration

This is the only official, 3GPP-standardized way of speaking a Gb interface over IP based transport.

It features the IP Sub-Network Service (IP-SNS) which allows either static configuration or dynamic configuration. The static configuration requires to specify the NSE and related NS-VC configuration via VTY similiar to Gb-over-FR.

##### 11.1.4.1 Gb over IP 3GPP auto-configuration

The auto-configuration allow to dynamically exchange information about IP endpoints (IP+port tuples) between the Gb interface peers. This means that normally only one initial IP endpoint needs to be configured. All additional IP endpoints and their relative weight for load distribution are then negotiated via the IP-SNS auto-configuration procedure.

The major differences of this true IP based Gb compared to any of the above are:

- No use of the NS-RESET, NS-BLOCK or NS-UNBLOCK procedures.
- Ability to use some NS-VCs only for signaling (data_weight=0) or only for user plane traffic (signaling_weight=0). This helps with SGSNs that have an internal control/user plane separation architecture.

Once the IP endpoints of the peers are known to each other, A full mesh of NS-VCs between all BSS endpoints and all SGSN endpoints is established.

Figure 3 below illustrates a deployment with two IP endpoints on both the BSS (PCU) and the SGSN, as well as the resulting four NS-VCs established between them.

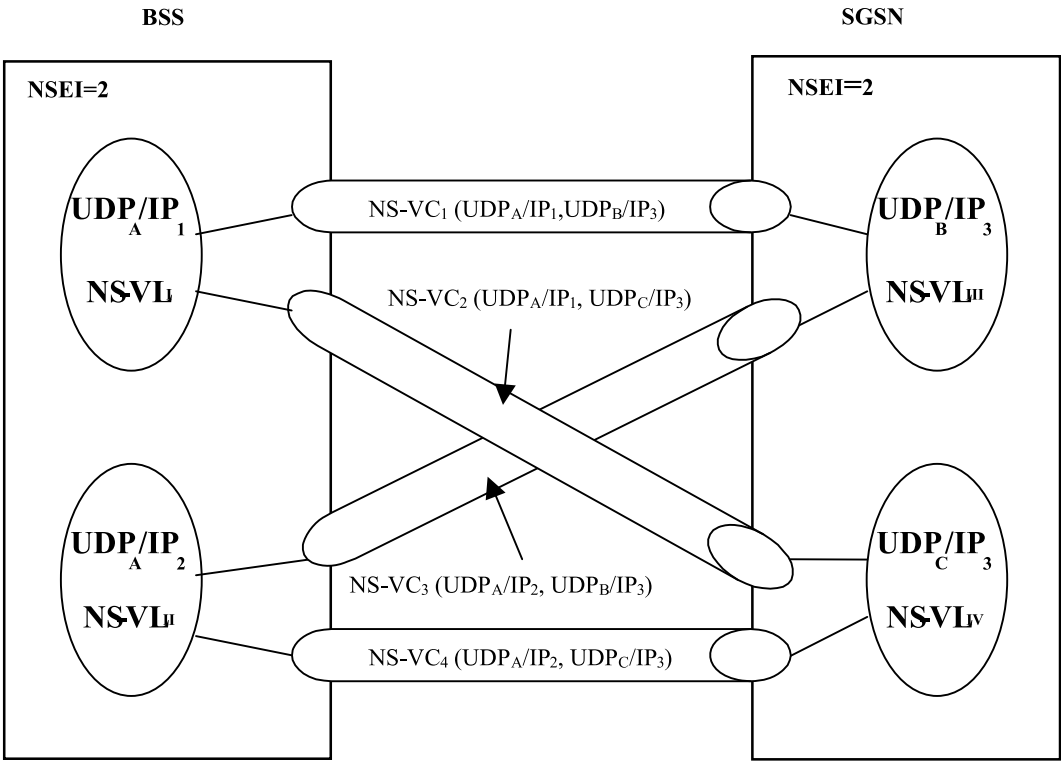



Figure 3: IP sub-network relationship between NS-VCs and NS-VLs (from 3GPP TS 48.016)

The sequence of messages in an IP-SNS enabled Gb interface bring-up can be seen in Figure 4. Here we have a PCU/BSS with a single IP endpoint and a SGSN with two IP endpoints, which results in only two NS-VC being established.

Furthermore, for each of the cells in the BSS/PCU, we can see the BVC-RESET procedure for its corresponding PTP BVC.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

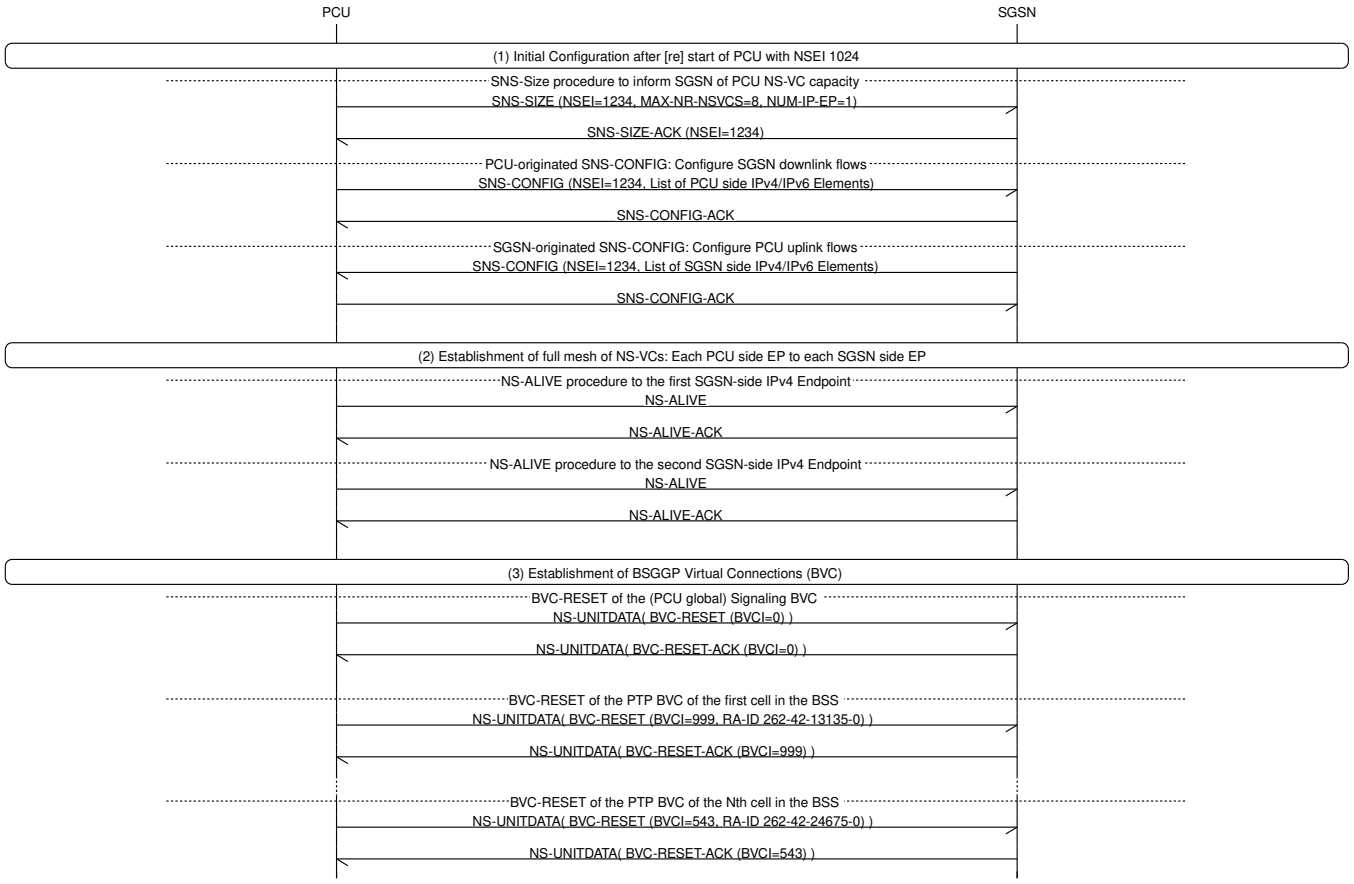



Figure 4: Initialization of Gb interface using IP-SNS procedures

## 11.2 General structure

The general structure of the configuration is split into 3 parts

- binds (NS-VL)
- nse (NS-E)
- timeouts

### 11.2.1 bind (NS-VL)

A bind represent a NS-VL. A bind has a specific type (IP/UDP or FR) and a unique name.

### 11.2.2 NS-E

A NSE node represents a NS Entity. A NSE is either persistent or dynamic. A persistent NSE is configured by VTY. A dynamic NSE is created on-demand without any VTY node. The SGSN/GbProxy creates dynamic NSE when a BSS connects to the SGSN (see accept-ipaccess). The PCU creates a dynamic NSE when it receives the configuration from BTS/BSC.

### 11.2.3 NS-VC

A NS-VC is always bound to a NSE and the bind (NS-VL). The NSVC can be either persistent or dynamic.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

## 11.3 Gb/NS configuration

This section describes the configuration that libosmogb exposes via the VTY and is valid for OsmoSGSN and OsmoGbProxy.

### 11.3.1 Gb over Frame Relay over E1/T1

The Gb over Frame Relay over E1/T1 requires:

- a hdlc interface
- a frame relay role (fr or frnet)
- the DLCI

**Example: Gb over Frame Relay configuration #1**

```
ns
 bind fr sitea1 ❶
  fr hdlc1 frnet ❷
 nse 2001 ❸
  nsvci fr sitea1 dlci 16 nsvci 11
```

❶ a Gb-over-FR bind with the name sitea1

❷ connect the hdlc1 device with the role frnet to sitea1

❸ one NSE (2001) with a single NS-VCI 11 on sitea1 with DLCI 16

**Example: Gb over Frame Relay configuration #2**

```
ns
 bind fr sitea1 ❶
  fr hdlc1 frnet ❷
 bind fr sitea2
  fr hdlc2 frnet
 bind fr sitea3
  fr hdlc3 frnet
 bind fr sitea4
  fr hdlc4 frnet
 bind fr siteb1
  fr hdlc5 frnet
 bind fr siteb2
  fr hdlc6 frnet
 bind fr sitec1
  fr hdlc7 frnet
 bind fr sitec2
  fr hdlc8 frnet
 nse 2001 ❸
  nsvci fr sitea1 dlci 16 nsvci 11
  nsvci fr sitea2 dlci 17 nsvci 12
  nsvci fr sitea3 dlci 18 nsvci 13
  nsvci fr sitea4 dlci 19 nsvci 14
 nse 2002 ❹
  nsvci fr siteb5 dlci 20 nsvci 15
  nsvci fr siteb6 dlci 21 nsvci 16
 nse 2003 ❺
  nsvc fr sitec7 dlci 22 nsvci 17
  nsvc fr sitec8 dlci 23 nsvci 18
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

1. a Gb-over-FR bind with the name sitea1
2. connect the hdlc1 device with the role frnet to sitea1
3. one NSE (2001) with four NS-VCI (11..14) on sitea1..4 with their respective DLCI
4. another NSE (2002) with two NS-VCI (15..16) on siteb1..2 with their respective DLCI
5. another NSE (2003) with two NS-VCI (17..18) on sitec1..2 with their respective DLCI

### 11.3.2 Gb over IP "ip.access style"

The Gb over IP "ip.access style" can be used with a dynamic configuration or with a static configuration

The static configuration requires to configure all endpoints on the BSS and SGSN. In contrast the dynamic configuration allows the SGSN to have only a reduced configuration.

#### 11.3.2.1 Gb over IP "ip.access style" dynamic configuration

**Example: Gb over IP/UDP ip.access style dynamic configuration (SGSN)**

```
ns
 bind udp ran1 ❶
  listen 10.100.1.1 23000 ❷
  accept-ipaccess ❸
```

1. create a IP/UDP bind with name ran1
2. bind to 10.100.1.1:23000
3. accept unknown BSS of ip.access style

**Example: Gb over IP/UDP "ip.access style" dynamic configuration (GbProxy as BSS)**

```
ns
 bind udp ran1 ❶
  listen 10.100.0.1 23000 ❷
 nse 1001 ❸
  nsvc ipa ran1 10.100.1.1 23000 nsvci 1001
```

1. create a IP/UDP bind with name ran1
2. bind to 10.100.1.1:23000
3. accept unknown BSS of ip.access style

**Note**
The OsmoPCU supports ip.access style Gb/NS but doesn't support this vty configuration because it's receiving the configuration from the BTS/BSC.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 11.3.2.2 Gb over IP "ip.access style" static configuration

**Example: Gb over IP/UDP "ip.access style" static configuration (BSS & SGSN)**

```
ns
 bind udp ran1 ❶
  listen 10.100.0.1 23000 ❷
 nse 1001 ❸
  nsvc ipa ran1 10.100.1.1 23000 nsvci 1001
```

❶ create a IP/UDP bind with name ran1

❷ bind to 10.100.0.1:23000

❸ NSE 1001 with nsvc 1001 as ip.access style

---

**Note**
The OsmoPCU supports "ip.access style" Gb/NS but doesn't support this vty configuration because it's receiving the configuration from the BTS/BSC.

---

### 11.3.3 Gb over IP 3GPP static configuration

A static IP/UDP configuration without SNS as specified by 3GPP 48.016.

**Example: Gb over IP/UDP static configuration BSS/SGSN**

```
ns
 bind udp ran1 ❶
  listen 10.100.0.1 23000 ❷
 nse 1001 ❸
  nsvc udp ran1 10.100.1.1 23000 signalling-weight 2 data-weight 2
  nsvc udp ran1 10.100.1.2 23000 ❹
```

❶ create a IP/UDP bind with name ran1

❷ bind to 10.100.0.1:23000

❸ add NSE 1001 with 2 NSVC

❹ short configuration with default signalling and data weight of 1

### 11.3.4 Gb over IP 3GPP auto configuration as BSS

IP/UDP auto-configuration with initial endpoints to an SGSN. The auto-configuration will use the first bind to connect to the first endpoint. If this fails Osmocom will iterate over all endpoints and binds to find a working combination.

**Example: Gb over IP/UDP auto-configuration as BSS**

```
ns
 bind udp ran1 ❶
  listen 10.100.0.1 23000 ❷
 bind udp ran2
  listen 10.100.0.2 23000
 bind udp ran3
  listen 10.100.0.3 23000
 nse 1001 ❸
  ip-sns-bind ran1 ❹
  ip-sns-bind ran2
  ip-sns-remote 10.100.1.1 23000 ❺
  ip-sns-remote 10.100.1.2 23000
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

1. create a IP/UDP bind with name ran1
2. bind to 10.100.0.1:23000
3. add NSE 1001 with 2 initial SNS endpoints
4. add ran1 to the list of available endpoints
5. add 10.100.1.1 as initial endpoint

### 11.3.5 Gb/NS Timer configuration

The NS protocol features a number of configurable timers.

Table 7: List of configurable NS timers

| | |
|---|---|
| tns-block | (un)blocking timer timeout (secs) |
| tns-block-retries | (un)blocking timer; number of retries |
| tns-reset | reset timer timeout (secs) |
| tns-reset-retries | reset timer; number of retries |
| tns-test | test timer timeout (secs) |
| tns-alive | alive timer timeout (secs) |
| tns-alive-retries | alive timer; number of retries |
| tsns-prov | SNS provision timeout (secs) used by all SNS auto configuration procedures. |
| tsns-size-retries | SNS Size procedure; number of retries |
| tsns-config-retries | SNS Config procedure; number of retries |

All timer can be configured by vty configuration

**Example of timeouts**

```
ns
 timer tns-block 3
 timer tns-block-retries 3
 timer tns-reset 3
 timer tns-reset-retries 3
 timer tns-test 30
 timer tns-alive 3
 timer tns-alive-retries 10
 timer tsns-prov 10
 timer tsns-size-retries 3
 timer tsns-config-retries 3
```

## 11.4 Gb/NS maintenance

This section describes common maintenance procedures.

### 11.4.1 NSE states

A NSE can have the following states:

NSE STATES

- ALIVE

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

- DEAD

For FR, IPA: The NSE is ALIVE if there is at least one NSVC in state UNBLOCKED. For IP-SNS/UDP: The NSE is ALIVE if there is at least one NSVC ALIVE and the sum of all ALIVE NSVCs signalling weights > 0 and data weights > 0.

The state of the NSE is shown by vty.

**show ns**

```
GbProxy# show ns nsei 1234
NSEI 01234: UDP, DEAD ❶
 FSM Instance Name: 'GPRS-NS2-SNS-BSS(NSE01234-SNS)[0x6120000012a0]', ID: 'NSE01234-SNS'
  Log-Level: 'DEBUG', State: 'BSS_SIZE'
  Timer: 1
 Maximum number of remote  NS-VCs: 8192, IPv4 Endpoints: 8192, IPv6 Endpoints: 8192
  1 NS-VC:
   NSVCI none: DISABLED DYNAMIC data_weight=1 sig_weight=1 udp) ↩
       [127.0.0.1]:23000<>[127.0.0.1]:22000
```

❶ NSE state

### 11.4.2 NSVC states

A NSVC can have the following states:

Table 8: nsvc states

| State | transport UNITDATA | Description |
|---|---|---|
| DISABLED | No | Either the transport layer is unavailable (FR) or this NSVC is currently used by IP-SNS dynamic configuration. |
| RESET | No | Sending out RESET PDU and awaiting data. |
| BLOCKED | No* | The NSVC has been BLOCKED. * see 3GPP TS 48.016 § 7.2 exception |
| UNBLOCKED/ALIVE | Yes | The NSVC transport UNITDATA. |
| RECOVERING | No | The NSVC test procedure timed out. NSVC type is a IP-SNS which don't use RESET/BLOCK/UNBLOCK. |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

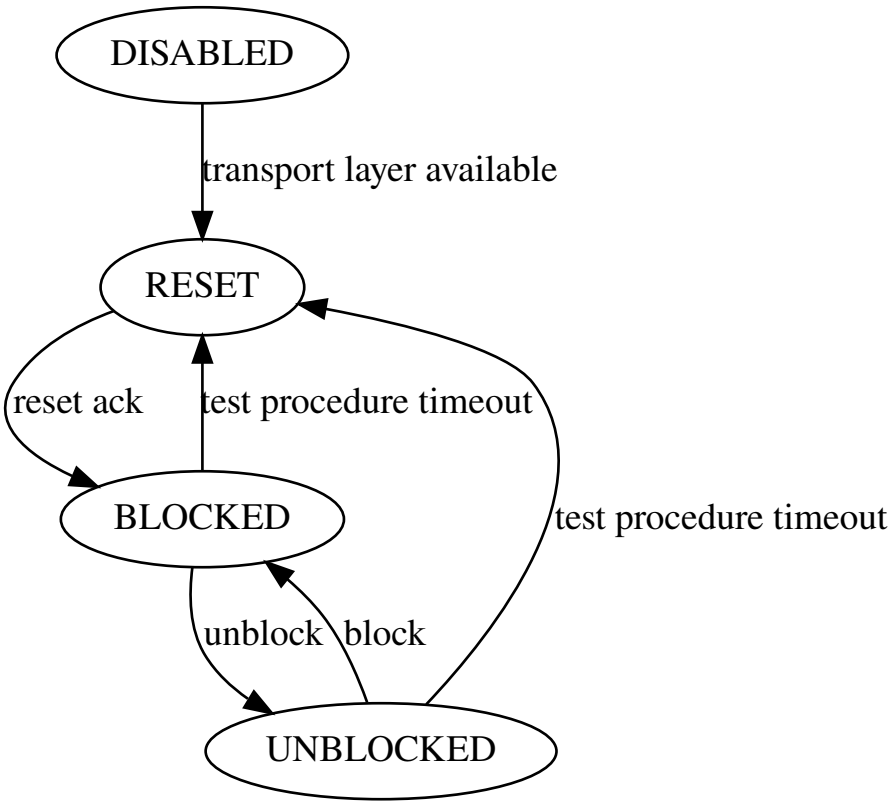



Figure 5: Simplified state diagram for RESET BLOCK UNBLOCK NSVCs

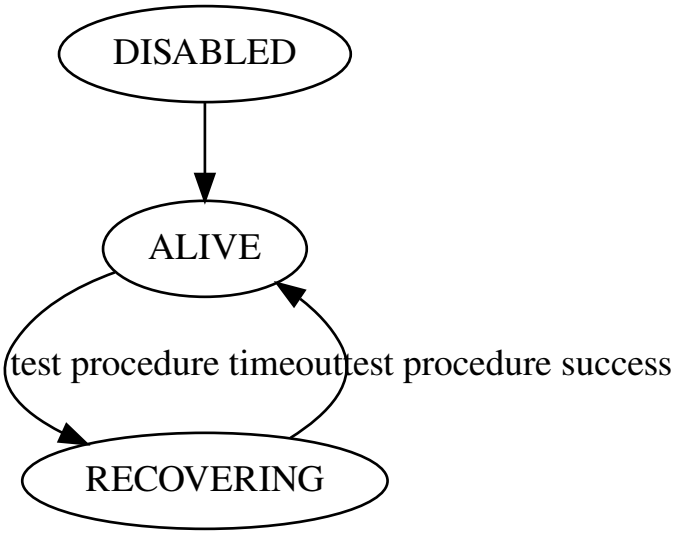



Figure 6: Simplified state diagram for IP-SNS/UDP

#### 11.4.3 Show information of a specific NSE

The NSE 1234 has been configured for as BSS with IP-SNS configuration.

**show ns on a dynamic configured IP-SNS NSE**

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

```
GbProxy# show ns nsei 1234
NSEI 01234: UDP, DEAD ❶
 FSM Instance Name: 'GPRS-NS2-SNS-BSS(NSE01234-SNS)[0x6120000012a0]', ID: 'NSE01234-SNS'
  Log-Level: 'DEBUG', State: 'BSS_SIZE' ❷
  Timer: 1
 Maximum number of remote  NS-VCs: 8192, IPv4 Endpoints: 8192, IPv6 Endpoints: 8192
  1 NS-VC:
   NSVCI none: DISABLED DYNAMIC data_weight=1 sig_weight=1 udp) ↩
       [127.0.0.1]:23000<>[127.0.0.1]:22000
```

❶ A UDP NSE. A NSE can be ALIVE or DEAD

❷ The SNS state. CONFIGURED and LOCAL_PROCEDURE are ALIVE states

For description of NSE states see Section 11.4.1.

**show ns on a frame relay NSE**

```
OsmoNSdummy# show ns nsei 02001
NSEI 02001: FR, ALIVE ❶
  4 NS-VC:
   NSVCI 00001: DISABLED PERSIST data_weight=1 sig_weight=1 fr)netif: hdlcnet1 dlci: 16 ❷
   NSVCI 00002: DISABLED PERSIST data_weight=1 sig_weight=1 fr)netif: hdlcnet2 dlci: 17 ❸
   NSVCI 00003: DISABLED PERSIST ❹ data_weight=1 sig_weight=1 fr)netif: hdlcnet3 dlci: 18
   NSVCI 00004: DISABLED PERSIST data_weight=1 sig_weight=1 fr)netif: hdlcnet4 dlci: 19
```

❶ A FR NSE. A NSE can be ALIVE or DEAD

❷ An unblocked NS-VC will be used for data and signalling. data and signalling weight are only relevant for UDP NSVC.

❸ NSVC is still blocked.

❹ A PERSIST NSVC is a configured via VTY.

### 11.4.4 Blocking a NSVC

**how to block a single NSVC**

```
OsmoNSdummy# show ns nsei 01234
NSEI 01234: UDP, ALIVE since 0d 0h 41m 6s
  2 NS-VC:
   NSVCI 01234: UNBLOCKED PERSIST udp)[127.0.0.1]:23000<1234>[127.0.0.1]:22000 ALIVE since ↩
       0d 0h 2m 36s
   NSVCI 01235: UNBLOCKED PERSIST udp)[127.0.0.1]:23001<1235>[127.0.0.1]:22001 ALIVE since ↩
       0d 0h 41m 6s

OsmoNSdummy# nsvc 1234 block
The NS-VC 01234 will be blocked.
OsmoNSdummy# show ns nsei 01234
NSEI 01234: UDP, ALIVE since 0d 0h 42m 7s
  2 NS-VC:
   NSVCI 01234: BLOCKED PERSIST udp)[127.0.0.1]:23000<1234>[127.0.0.1]:22000 DEAD since 0d ↩
       0h 3m 37s
   NSVCI 01235: UNBLOCKED PERSIST udp)[127.0.0.1]:23001<1235>[127.0.0.1]:22001 ALIVE since ↩
       0d 0h 42m 7s
```

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

# 12 Osmocom Control Interface

The VTY interface as described in Section 7 is aimed at human interaction with the respective Osmocom program.

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

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

## 12.1 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).

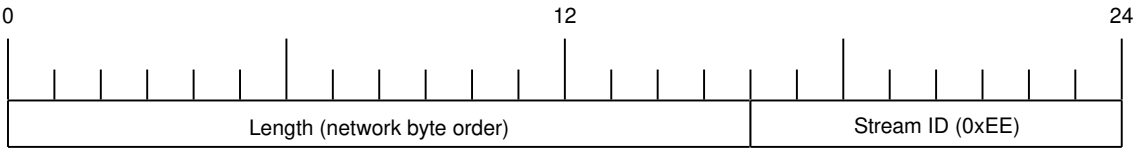



Figure 7: IPA header for control protocol

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

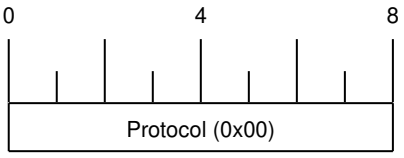



Figure 8: IPA extension header for control protocol

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.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

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

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

#### 12.1.1 GET operation

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

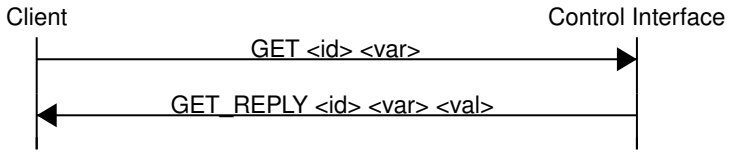



Figure 9: Control Interface GET operation (successful outcome)

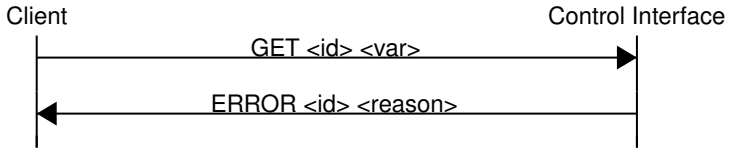



Figure 10: Control Interface GET operation (unsuccessful outcome)

#### 12.1.2 SET operation

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

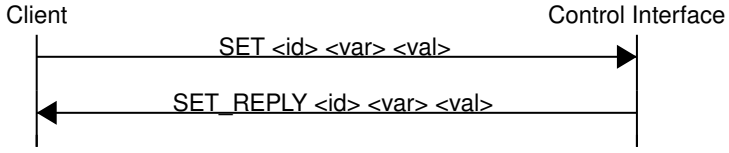



Figure 11: Control Interface SET operation (successful outcome)

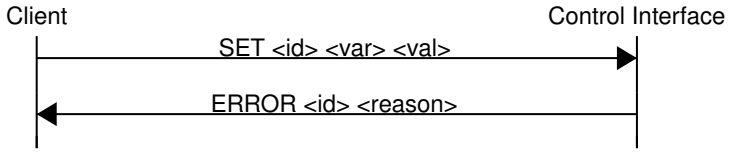



Figure 12: Control Interface SET operation (unsuccessful outcome)

#### 12.1.3 TRAP operation

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

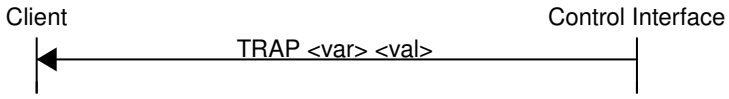



Figure 13: Control Interface TRAP operation

## 12.2 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.

## 12.3 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 12.2 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.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 12.3.1 Getting rate counters

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

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

#### 12.3.2 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
```

#### 12.3.3 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
```

#### 12.3.4 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

## 13 Osmocom Authentication Protocol (OAP)

### 13.1 General

The Osmocom Authentication Protocol employs mutual authentication to register a client with a server over an IPA connection. Milenage is used as the authentication algorithm, where client and server have a shared secret.

For example, an SGSN, as OAP client, may use its SGSN ID to register with a MAP proxy, an OAP server.

Copyright © 2013-2024 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).

## 13.3 Using IPA

By default, the following identifiers should be used: - IPA protocol: 0xee (OSMO) - IPA OSMO protocol extension: 0x06 (OAP)

## 13.4 Procedures

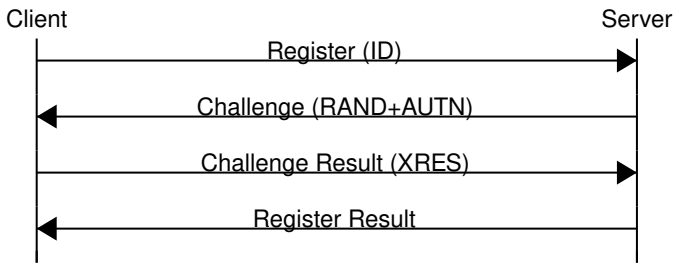



Figure 14: Ideal communication sequence

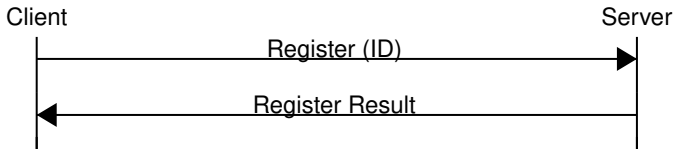



Figure 15: Variation "test setup"

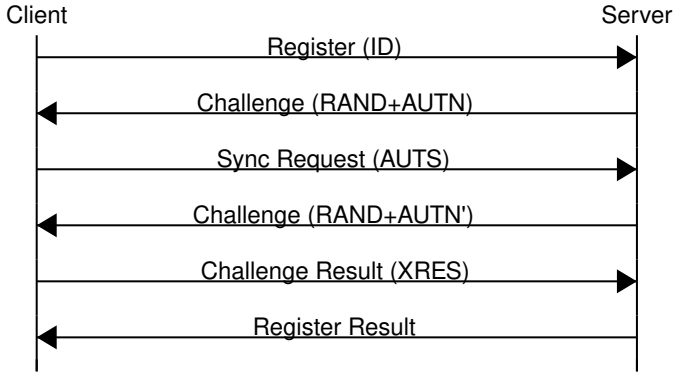



Figure 16: Variation "invalid sequence nr":

### 13.4.1 Register

The client sends a REGISTER_REQ message containing an identifier number.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 13.4.2 Challenge

The OAP server (optionally) sends back a CHALLENGE_REQ, containing random bytes and a milenage authentication token generated from these random bytes, using a shared secret, to authenticate itself to the OAP client. The server may omit this challenge entirely, based on its configuration, and immediately reply with a Register Result response. If the client cannot be registered (e.g. id is invalid), the server sends a REGISTER_ERR response.

#### 13.4.3 Challenge Result

When the client has received a Challenge, it may verify the server's authenticity and validity of the sequence number (included in AUTN), and, if valid, reply with a CHALLENGE_RES message. This shall contain an XRES authentication token generated by milenage from the same random bytes received from the server and the same shared secret. If the client decides to cancel the registration (e.g. invalid AUTN), it shall not reply to the CHALLENGE_REQ; a CHALLENGE_ERR message may be sent, but is not mandatory. For example, the client may directly start with a new REGISTER_REQ message.

#### 13.4.4 Sync Request

When the client has received a Challenge but sees an invalid sequence number (embedded in AUTN, according to the milenage algorithm), the client may send a SYNC_REQ message containing an AUTS synchronisation token.

#### 13.4.5 Sync Result

If the server has received a valid Sync Request, it shall answer by directly sending another Challenge (see Section 13.4.2). If an invalid Sync Request is received, the server shall reply with a REGISTER_ERR message.

#### 13.4.6 Register Result

The server sends a REGISTER_RES message to indicate that registration has been successful. If the server cannot register the client (e.g. invalid challenge response), it shall send a REGISTER_ERR message.

### 13.5 Message Format

Every message is based on the following message format

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |

The receiver shall be able to receive IEs in any order. Unknown IEs shall be ignored.

#### 13.5.1 Register Request

Direction: Client → Server

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |
| 30 | Client ID | Section 13.6.3 | M | TLV | 4 |

#### 13.5.2 Register Error

Direction: Server → Client

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |
| 02 | Cause | GMM Cause, TS 24.008: 10.5.5.14 | M | TLV | 3 |

#### 13.5.3 Register Result

Direction: Server → Client

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |

#### 13.5.4 Challenge

Direction: Server → Client

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |
| 20 | RAND | octet string (16) | TLV | 18 | 23 |

#### 13.5.5 Challenge Error

Direction: Client → Server

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |
| 02 | Cause | GMM Cause, TS 24.008: 10.5.5.14 | M | TLV | 3 |

#### 13.5.6 Challenge Result

Direction: Client → Server

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |

#### 13.5.7 Sync Request

Direction: Client → Server

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 13.6.1 | M | V | 1 |

#### 13.5.8 Sync Error

Not used.

#### 13.5.9 Sync Result

Not used.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

## 13.6 Information Elements

### 13.6.1 Message Type

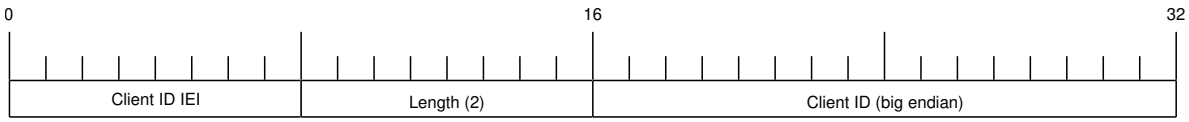
| **0x04** | **Register Request** |
|---|---|
| 0x05 | Register Error |
| 0x06 | Register Result |
| 0x08 | Challenge Request |
| 0x09 | Challenge Error |
| 0x0a | Challenge Result |
| 0x0c | Sync Request |
| 0x0d | Sync Error (not used) |
| 0x0e | Sync Result (not used) |

### 13.6.2 IE Identifier (informational)

These are the standard values for the IEI.

| **IEI** | **Info Element** | **Type** |
|---|---|---|
| 0x02 | Cause | GMM Cause, 04.08: 10.5.5.14 |
| 0x20 | RAND | Octet String |
| 0x23 | AUTN | Octet Strong |
| 0x24 | XRES | Octet String |
| 0x25 | AUTS | Octet String |
| 0x30 | Client ID | big endian integer, 16 bit |

### 13.6.3 Client ID




The Client ID number shall be interpreted as an unsigned 16bit integer, where 0 indicates an invalid / unset ID.

# 14 Generic Subscriber Update Protocol

## 14.1 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:

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

- 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.

## 14.2 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.

## 14.3 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*.

## 14.4 Procedures

### 14.4.1 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)

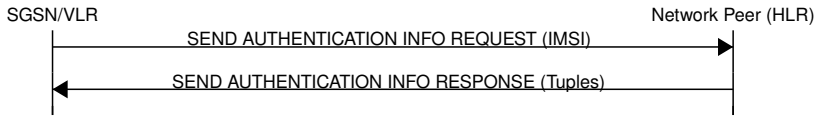



Figure 17: Send Authentication Info (Normal Case)

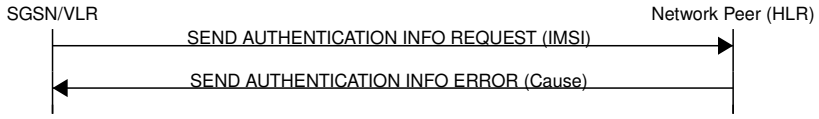



Figure 18: Send Authentication Info (Erroneous Case)

### 14.4.2 Reporting of Authentication Failure

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

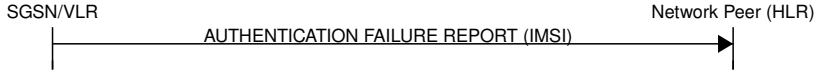



Figure 19: Authentication Failure Report (Normal Case)

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 14.4.3 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)

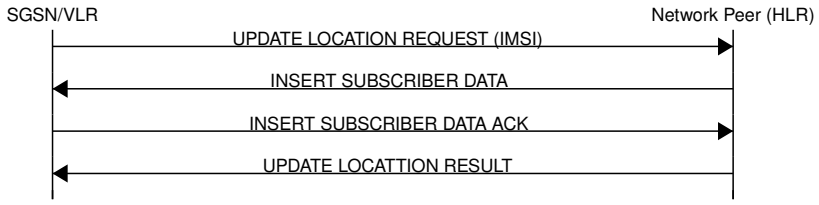



Figure 20: Update Location (Normal Case)

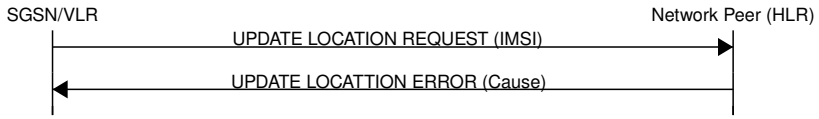



Figure 21: Update Location (Error Case)

### 14.4.4 Location Cancellation

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

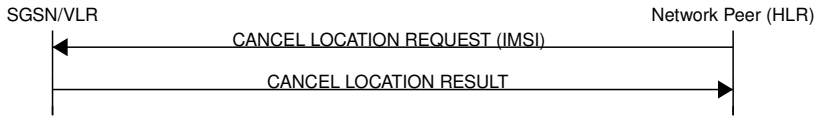



Figure 22: Cancel Location (Normal Case)

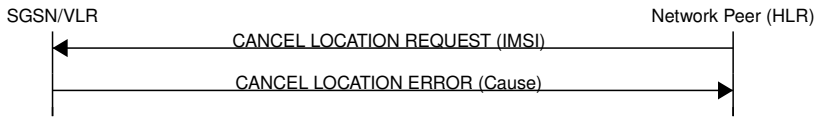



Figure 23: Cancel Location (Error Case)

### 14.4.5 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

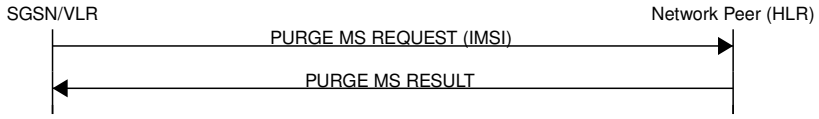



Figure 24: Purge MS (Normal Case)

#### 14.4.6 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.

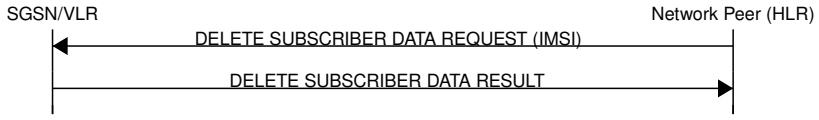



Figure 25: Delete Subscriber Data (Normal Case)

#### 14.4.7 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.

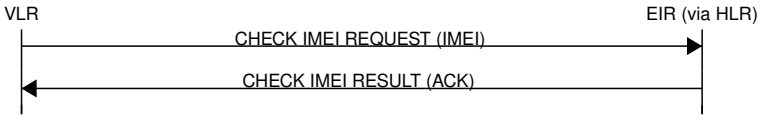



Figure 26: Check IMEI (Normal Case)

### 14.5 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.

#### 14.5.1 E Handover

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

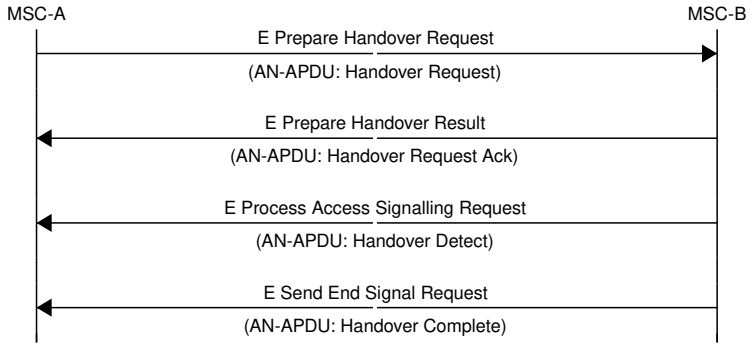



Figure 27: E Handover (Normal Case)

#### 14.5.2 E Subsequent Handover

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

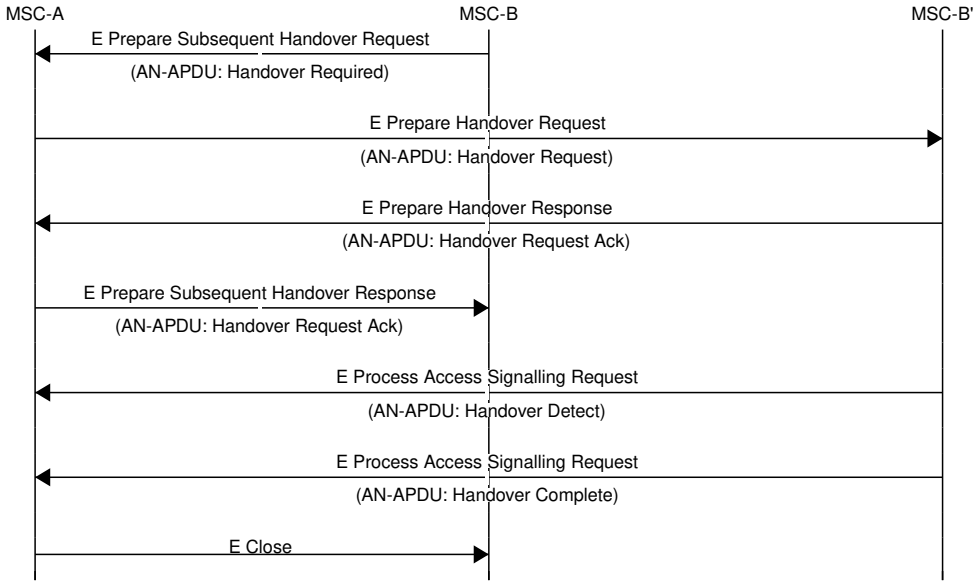



Figure 28: E Subsequent Handover (Normal Case)

#### 14.5.3 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.

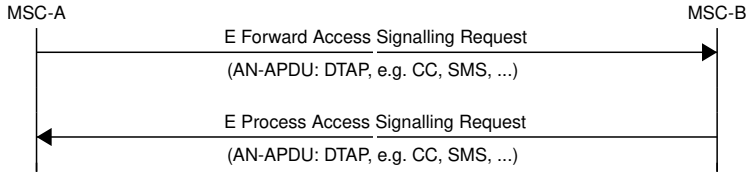



Figure 29: E Process and Forward Access Signalling (Normal Case)

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.5.4 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 14.7.31), 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.

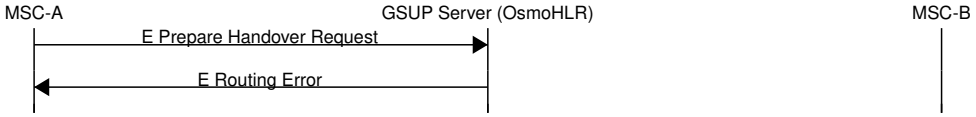



Figure 30: E Routing Error example

### 14.6 Message Format

#### 14.6.1 General

Every message is based on the following message format

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | 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).

#### 14.6.2 Send Authentication Info Request

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 26 | AUTS | Section 14.7.13 | C | TLV | 18 |
| 20 | RAND | Section 14.7.7 | C | TLV | 18 |
| 05 | PDP info | Section 14.7.3 | C | TLV | 2-N |

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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.6.3 Send Authentication Info Error

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.4 Send Authentication Info Response

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 03 | Auth Tuple | Section 14.7.6 | 0-5 | TLV | 36 |

#### 14.6.5 Authentication Failure Report

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |

#### 14.6.6 Update Location Request

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |

#### 14.6.7 Update Location Error

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.8 Update Location Result

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 08 | MSISDN | Section 14.7.20 | O | TLV | 0-9 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| 09 | HLR Number | Section 14.7.25 | O | TLV | 0-9 |
| 04 | PDP info complete | Section 14.7.18 | O | TLV | 2 |
| 05 | PDP info | Section 14.7.3 | O | TLV | 2-N |

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

#### 14.6.9 Location Cancellation Request

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 06 | Cancellation type | Section 14.7.16 | O | TLV | 3 |

#### 14.6.10 Location Cancellation Error

Direction: SGSN / VLR ⇒ HLR

TODO

#### 14.6.11 Location Cancellation Result

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |

#### 14.6.12 Purge MS Request

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 09 | HLR Number | Section 14.7.25 | M | TLV | 0-9 |

#### 14.6.13 Purge MS Error

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.6.14 Purge MS Result

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 07 | Freeze P-TMSI | Section 14.7.18 | M | TLV | 2 |

#### 14.6.15 Insert Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 08 | MSISDN | Section 14.7.20 | O | TLV | 0-9 |
| 09 | HLR Number | Section 14.7.25 | O | TLV | 0-9 |
| 04 | PDP info complete | Section 14.7.18 | M | TLV | 2 |
| 05 | PDP info | Section 14.7.3 | C | TLV | 0-10 |
| 14 | PDP-Charging Characteristics | Section 14.7.23 | O | TLV | 4 |

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

#### 14.6.16 Insert Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.17 Insert Subscriber Data Result

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |

#### 14.6.18 Delete Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 10 | PDP Context ID | Section 14.7.5 | C | TLV | 3 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.6.19 Delete Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.20 Delete Subscriber Data Result

Direction: HLR ⇒ SGSN / VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |

#### 14.6.21 Process Supplementary Service Request

Direction: bidirectional

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 30 | Session ID | Section 14.8.1 | M | TLV | 6 |
| 31 | Session State | Section 14.8.2 | M | TLV | 3 |
| 35 | Supplementary Service Info | Section 14.7.27 | 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.

#### 14.6.22 Process Supplementary Service Error

Direction: EUSE / HLR ⇒ MSC

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 30 | Session ID | Section 14.8.1 | M | TLV | 6 |
| 31 | Session State | Section 14.8.2 | M | TLV | 3 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.23 Process Supplementary Service Response

Direction: EUSE / HLR ⇒ MSC

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 30 | Session ID | Section 14.8.1 | M | TLV | 6 |
| 31 | Session State | Section 14.8.2 | M | TLV | 3 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| 35 | Supplementary Service Info | Section 14.7.27 | 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.

#### 14.6.24 MO-forwardSM Request

Direction: MSC / SGSN ⇒ SMSC (via HLR)

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | M | TLV | 1 |
| 41 | SM-RP-DA (Destination Address) | Section 14.8.4 | M | TLV | 2-... |
| 42 | SM-RP-OA (Originating Address) | Section 14.8.5 | M | TLV | 2-... |
| 43 | SM-RP-UI (SM TPDU) | Section 14.8.7 | 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.

#### 14.6.25 MO-forwardSM Error

Direction: SMSC (via HLR) ⇒ MSC / SGSN

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | M | TLV | 1 |
| 44 | SM-RP-Cause (Cause value) | Section 14.8.8 | M | TLV | 1 |
| 43 | SM-RP-UI (diagnostic field) | Section 14.8.7 | 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.

#### 14.6.26 MO-forwardSM Result

Direction: SMSC (via HLR) ⇒ MSC / SGSN

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.6.27 MT-forwardSM Request

Direction: SMSC (via HLR) ⇒ MSC / SGSN

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | M | TLV | 1 |
| 41 | SM-RP-DA (Destination Address) | Section 14.8.4 | M | TLV | 2-... |
| 42 | SM-RP-OA (Originating Address) | Section 14.8.5 | M | TLV | 2-... |
| 43 | SM-RP-UI (SM TPDU) | Section 14.8.7 | M | TLV | 1-... |
| 45 | SM-RP-MMS (More Messages to Send) | Section 14.8.9 | 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.

#### 14.6.28 MT-forwardSM Error

Direction: MSC / SGSN ⇒ SMSC (via HLR)

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | M | TLV | 1 |
| 44 | SM-RP-Cause (Cause value) | Section 14.8.8 | M | TLV | 1 |
| 43 | SM-RP-UI (diagnostic field) | Section 14.8.7 | 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.

#### 14.6.29 MT-forwardSM Result

Direction: MSC / SGSN ⇒ SMSC (via HLR)

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | 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.

#### 14.6.30 READY-FOR-SM Request

Direction: MSC / SGSN ⇒ SMSC (via HLR)

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | M | TLV | 1 |
| 46 | SM Alert Reason | Section 14.8.10 | 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.6.31 READY-FOR-SM Error

Direction: SMSC (via HLR) ⇒ MSC / SGSN

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | M | TLV | 1 |
| 44 | SM-RP-Cause (Cause value) | Section 14.8.8 | M | TLV | 1 |
| 43 | SM-RP-UI (diagnostic field) | Section 14.8.7 | 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.

#### 14.6.32 READY-FOR-SM Result

Direction: SMSC (via HLR) ⇒ MSC / SGSN

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 40 | SM-RP-MR (Message Reference) | Section 14.8.3 | 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.

#### 14.6.33 CHECK-IMEI Request

Direction: VLR ⇒ EIR (via HLR)

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 50 | IMEI | Section 14.7.28 | M | TLV | 11 |

#### 14.6.34 CHECK-IMEI Error

Direction: EIR (via HLR) ⇒ VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.35 CHECK-IMEI Result

Direction: EIR (via HLR) ⇒ VLR

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 51 | IMEI Check Result | Section 14.7.29 | M | TLV | 3 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.6.36 E Prepare Handover Request

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.37 E Prepare Handover Error

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.38 E Prepare Handover Result

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.39 E Prepare Subsequent Handover Request

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.40 E Prepare Subsequent Handover Error

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.41 E Prepare Subsequent Handover Result

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.42 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 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.43 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 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.44 E Send End Signal Result

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.45 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 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.46 E Forward Access Signalling Request

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 62 | AN-APDU | Section 14.7.33 | M | TLV | 2-... |

#### 14.6.47 E Close

Direction: MSC-A ⇒ MSC-B (via HLR)

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |

#### 14.6.48 E Abort

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

#### 14.6.49 E Routing Error

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | M | TLV | 2-... |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| 61 | Destination Name | Section 14.7.32 | M | TLV | 2-... |
| 30 | Session ID | Section 14.8.1 | O | TLV | 6 |
| 31 | Session State | Section 14.8.2 | O | TLV | 3 |

#### 14.6.50 ePDG Tunnel Request

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 15 | PCO | Section 14.7.24 | O | TLV | 1-... |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | O | TLV | 2-... |

#### 14.6.51 ePDG Tunnel Error

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 02 | Cause | Section 14.7.26 | M | TLV | 3 |

#### 14.6.52 ePDG Tunnel Result

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Message Type | Section 14.7.1 | M | V | 1 |
| 01 | IMSI | Section 14.7.19 | M | TLV | 2-10 |
| 0a | Message Class | Section 14.7.30 | M | TLV | 3 |
| 04 | PDP info complete | Section 14.7.18 | M | TLV | 2 |
| 05 | PDP info | Section 14.7.3 | M | TLV | 2-N |
| 15 | PCO | Section 14.7.24 | O | TLV | 1-... |
| 28 | CN Domain | Section 14.7.15 | O | TLV | 3 |
| 60 | Source Name | Section 14.7.31 | O | TLV | 2-... |

### 14.7 Information Elements

#### 14.7.1 Message Type

| Type | Name |
|---|---|
| Description | 0x04 |
| Update Location Request | Section 14.6.6 |
| 0x05 | Update Location Error |
| Section 14.6.7 | 0x06 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| Type | Name |
|---|---|
| Update Location Result | Section 14.6.8 |
| 0x08 | Send Authentication Info Request |
| Section 14.6.2 | 0x09 |
| Send Authentication Info Error | Section 14.6.3 |
| 0x0a | Send Authentication Info Result |
| Section 14.6.4 | 0x0b |
| Authentication Failure Report | Section 14.6.5 |
| 0x0c | Purge MS Request |
| [?] | 0x0d |
| Purge MS Error | Section 14.6.13 |
| 0x0e | Purge MS Result |
| Section 14.6.14 | 0x10 |
| Insert Subscriber Data Request | Section 14.6.15 |
| 0x11 | Insert Subscriber Data Error |
| Section 14.6.16 | 0x12 |
| Insert Subscriber Data Result | Section 14.6.17 |
| 0x14 | Delete Subscriber Data Request |
| Section 14.6.18 | 0x15 |
| Delete Subscriber Data Error | Section 14.6.19 |
| 0x16 | Delete Subscriber Data Result |
| Section 14.6.20 | 0x1c |
| Location Cancellation Request | Section 14.6.9 |
| 0x1d | Location Cancellation Error |
| Section 14.6.10 | 0x1e |
| Location Cancellation Result | Section 14.6.11 |
| 0x20 | Supplementary Service Request |
| Section 14.6.21 | 0x21 |
| Supplementary Service Error | Section 14.6.22 |
| 0x22 | Supplementary Service Result |
| Section 14.6.23 | 0x24 |
| MO-forwardSM Request | Section 14.6.24 |
| 0x25 | MO-forwardSM Error |
| Section 14.6.25 | 0x26 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| Type | Name |
|---|---|
| MO-forwardSM Result | Section 14.6.26 |
| 0x28 | MT-forwardSM Request |
| Section 14.6.27 | 0x29 |
| MT-forwardSM Error | Section 14.6.28 |
| 0x2a | MT-forwardSM Result |
| Section 14.6.29 | 0x2c |
| READY-FOR-SM Request | Section 14.6.30 |
| 0x2d | READY-FOR-SM Error |
| Section 14.6.31 | 0x2e |
| READY-FOR-SM Result | Section 14.6.32 |
| 0x30 | CHECK-IMEI Request |
| Section 14.6.33 | 0x31 |
| CHECK-IMEI Error | Section 14.6.34 |
| 0x32 | CHECK-IMEI Result |
| Section 14.6.35 | 0x34 |
| E Prepare Handover Request | Section 14.6.36 |
| 0x35 | E Prepare Handover Error |
| Section 14.6.37 | 0x36 |
| E Prepare Handover Result | Section 14.6.38 |
| 0x38 | E Prepare Subsequent Handover Request |
| Section 14.6.39 | 0x39 |
| E Prepare Subsequent Handover Error | Section 14.6.40 |
| 0x3a | E Prepare Subsequent Handover Result |
| Section 14.6.41 | 0x3c |
| E Send End Signal Request | Section 14.6.42 |
| 0x3d | E Send End Signal Error |
| Section 14.6.43 | 0x3e |
| E Send End Signal Result | Section 14.6.44 |
| 0x40 | E Process Access Signalling Request |
| Section 14.6.45 | 0x44 |
| E Forward Access Signalling Request | Section 14.6.46 |
| 0x47 | E Close |
| Section 14.6.47 | 0x4B |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

| Type | Name |
|---|---|
| E Abort | Section 14.6.48 |
| 0x4E | E Routing Error |
| Section 14.6.49 | 0x50 |
| ePDG Tunnel Request | Section 14.6.50 |
| 0x51 | ePDG Tunnel Error |
| Section 14.6.51 | 0x52 |
| ePDG Tunnel Result | Section 14.6.52 |

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 |

### 14.7.2 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*.

### 14.7.3 PDP Info

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

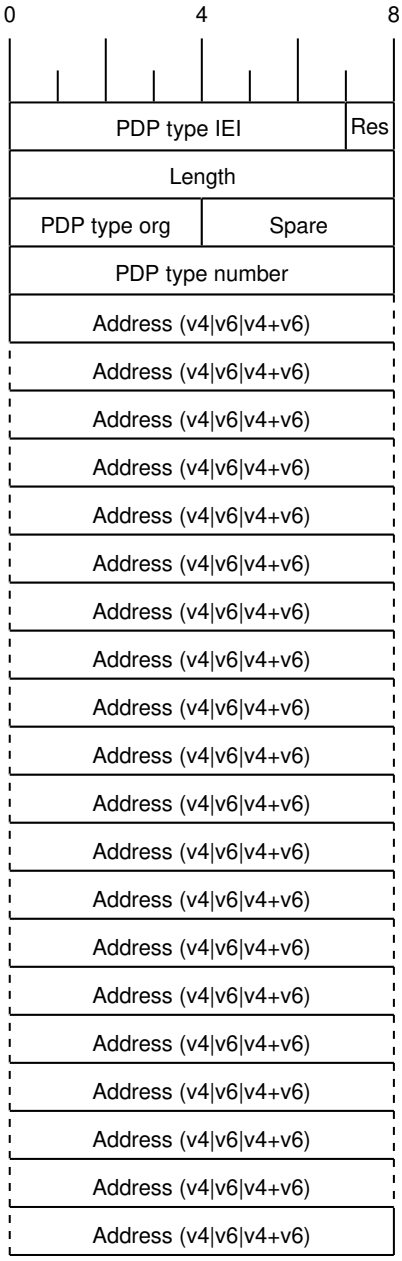
| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | PDP Info IEI | Section 14.7.17 | M | V | 1 |
| | Length of PDP Info IE | | M | V | 1 |
| 10 | PDP Context ID | Section 14.7.5 | C | TLV | 3 |
| 11 | PDP Address | Section 14.7.4 | C | TLV | 4-24 |
| 12 | Access Point Name | Section 14.7.21 | C | TLV | 3-102 |
| 13 | Quality of Service | Section 14.7.22 | O | TLV | 1-20 |
| 14 | PDP-Charging Characteristics | Section 14.7.23 | O | TLV | 4 |

The conditional IE are mandantory unless mentioned otherwise.

### 14.7.4 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 © 2013-2024 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.

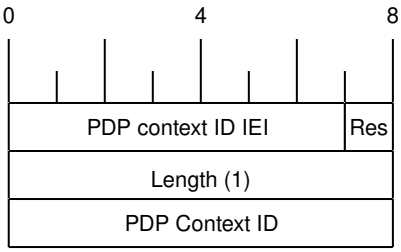
Examples:

- 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

### 14.7.5 PDP Context ID

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




### 14.7.6 Auth tuple

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

| IEI | IE | Type | Presence | Format | Length |
|---|---|---|---|---|---|
| | Auth Tuple IEI | Section 14.7.17 | M | V | 1 |
| | Length of Auth Tuple IE | | M | V | 1 |
| 20 | RAND | Section 14.7.7 | M | TLV | 18 |
| 21 | SRES | Section 14.7.8 | M | TLV | 6 |
| 22 | Kc | Section 14.7.9 | M | TLV | 10 |
| 23 | IK | Section 14.7.10 | C | TLV | 18 |
| 24 | CK | Section 14.7.11 | C | TLV | 18 |
| 25 | AUTN | Section 14.7.12 | C | TLV | 18 |
| 27 | RES | Section 14.7.14 | C | TLV | 2-18 |

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

### 14.7.7 RAND

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

### 14.7.8 SRES

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

### 14.7.9 Kc

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

### 14.7.10 IK

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.7.11 CK

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

#### 14.7.12 AUTN

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

#### 14.7.13 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.

#### 14.7.14 RES

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

#### 14.7.15 CN Domain

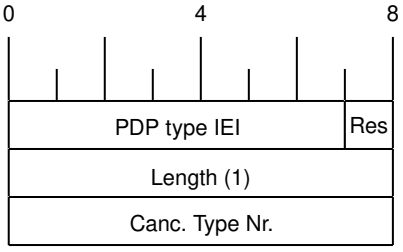
This single-byte information element indicates the Core Network Domain, i.e. if the message is related to Circuit Switched or Packet Switched services.

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

Table 74: CN Domain Number

| Type | Description |
|---|---|
| 0x01 | PS Domain |
| 0x02 | CS Domain |

#### 14.7.16 Cancellation Type




Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

Table 75: Cancellation Type Number

| Number | Description |
|---|---|
| 0x00 | Update Procedure |
| 0x01 | Subscription Withdrawn |

#### 14.7.17 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 76: GSUP IE Identifiers

| IEI | Info Element | Type / Encoding |
|---|---|---|
| 0x01 | IMSI | Mobile Identity, 3GPP TS 24.008 Ch. 10.5.1.4 |
| 0x02 | Cause | Section 14.7.26 |
| 0x03 | Auth Tuple | Section 14.7.6 |
| 0x04 | PDP Info Compl | Section 14.7.18 |
| 0x05 | PDP Info | Section 14.7.3 |
| 0x06 | Cancel Type | Section 14.7.16 |
| 0x07 | Freeze P-TMSI | Section 14.7.18 |
| 0x08 | MSISDN | ISDN-AddressString/octet, Section 14.7.20 |
| 0x09 | HLR Number | Section 14.7.25 |
| 0x0a | Message Class | Section 14.7.30 |
| 0x10 | PDP Context ID | Section 14.7.5 |
| 0x11 | PDP Address | [?] |
| 0x12 | Access Point Name | Section 14.7.21 |
| 0x13 | QoS | Section 14.7.22 |
| 0x14 | PDP-Charging Characteristics | Section 14.7.23 |
| 0x15 | PCO | Section 14.7.24 |
| 0x20 | RAND | Section 14.7.7 |
| 0x21 | SRES | Section 14.7.8 |
| 0x22 | Kc | Section 14.7.9 |
| 0x23 | IK | Section 14.7.10 |
| 0x24 | CK | Section 14.7.11 |
| 0x25 | AUTN | Section 14.7.12 |
| 0x26 | AUTS | Section 14.7.13 |
| 0x27 | RES | Section 14.7.14 |
| 0x28 | CN Domain | Section 14.7.15 |
| 0x30 | Session ID | Section 14.8.1 |
| 0x31 | Session State | Section 14.8.2 |
| 0x35 | Supplementary Service Info | Section 14.7.27 |
| 0x40 | SM-RP-MR (Message Reference) | Section 14.8.3 |
| 0x41 | SM-RP-DA (Destination Address) | Section 14.8.4 |
| 0x42 | SM-RP-OA (Originating Address) | Section 14.8.5 |
| 0x43 | SM-RP-UI (SM TPDU) | Section 14.8.7 |
| 0x44 | SM-RP-Cause (RP Cause value) | Section 14.8.8 |
| 0x45 | SM-RP-MMS (More Messages to Send) | Section 14.8.9 |
| 0x46 | SM Alert Reason | Section 14.8.10 |
| 0x50 | IMEI | Section 14.7.28 |
| 0x51 | IMEI Check Result | Section 14.7.29 |
| 0x60 | Source Name | Section 14.7.31 |
| 0x61 | Destination Name | Section 14.7.32 |
| 0x62 | AN-APDU | Section 14.7.33 |

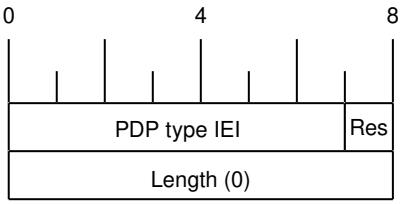
Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

Table 76: (continued)

| IEI | Info Element | Type / Encoding |
|---|---|---|
| 0x63 | RR Cause | Section 14.7.34 |
| 0x64 | BSSAP Cause | Section 14.7.35 |
| 0x65 | Session Management Cause | Section 14.7.36 |

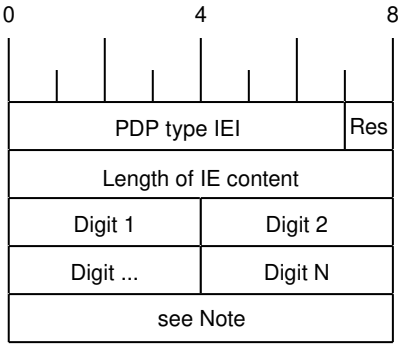
#### 14.7.18 Empty field

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.




#### 14.7.19 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.



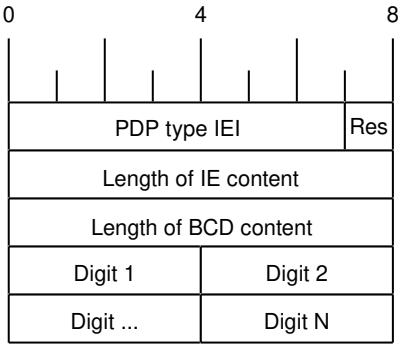

**Note**
Either *1 1 1 1* | *Number digit N* (N odd) or *Number digit N* | *Number digit N-1* (N even), where N is the number of digits.

#### 14.7.20 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

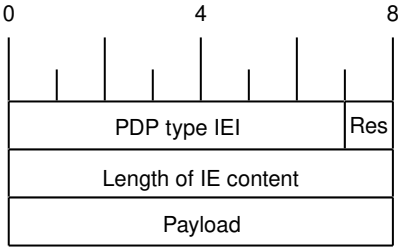



#### 14.7.21 Access Point Name

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

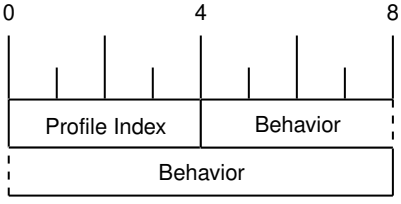
#### 14.7.22 Quality of Service Subscribed Service

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.




#### 14.7.23 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.



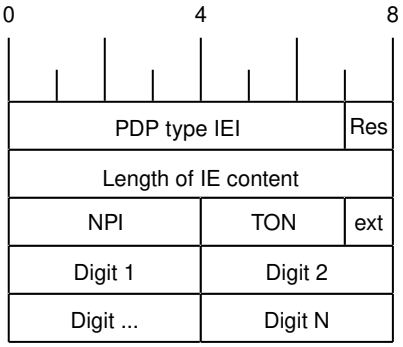

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.7.24 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.

#### 14.7.25 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.




#### 14.7.26 Cause

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

#### 14.7.27 Supplementary Service Info

This IE shall be used together with both Section 14.8.2 and Section 14.8.1 IEs. It is used to carry the payload of Supplementary Services encoded according to GSM TS 04.80.

#### 14.7.28 IMEI

The IMEI encoded as Called Party BCD Number in 3GPP TS 24.008. This IE has the same format as described in Section 14.7.20.

#### 14.7.29 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 77: IMEI Check Result

| Type | Description |
|---|---|
| 0x01 | ACK |
| 0x02 | NACK |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.7.30 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 |

#### 14.7.31 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.

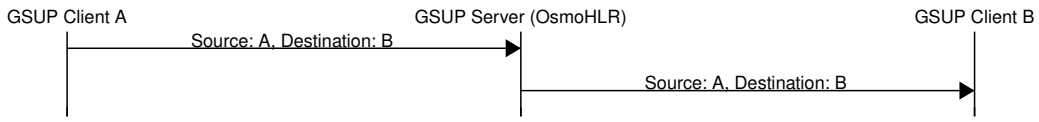



Figure 31: Message forwarding example

#### 14.7.32 Destination Name

The receiving counterpart to source name (Section 14.7.31).

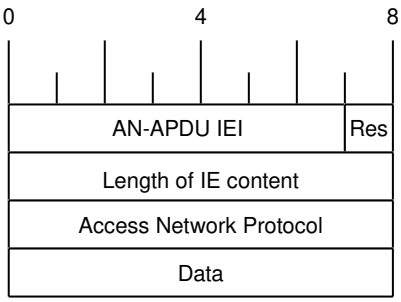
#### 14.7.33 AN-APDU

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

Table 79: Access Network Protocol

| Type | Description |
|---|---|
| 0x01 | BSSAP |
| 0x02 | RANAP |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 




#### 14.7.34 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.

#### 14.7.35 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.

#### 14.7.36 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.

### 14.8 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.

#### 14.8.1 Session ID

This auxiliary IE shall be used together with Section 14.8.2. The purpose of this IE is to identify a particular transaction using the 4-byte unique identifier.

#### 14.8.2 Session State

This auxiliary IE shall be used together with Section 14.8.1. The purpose of this IE is to indicate a state of a particular transacrion, i.e. initiate, continue or terminate it.

Table 80: 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 |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.8.3 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 14.8.3 is used to carry the message reference value 'as-is' (i.e. in range 0 through 255).

#### 14.8.4 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 14.8.6. See 3GPP TS 29.002, section 7.6.8.1 for details.

#### 14.8.5 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 14.8.6. See 3GPP TS 29.002, section 7.6.8.2 for details.

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

Basically, both Section 14.8.4 / Section 14.8.5 IEs contain a single TV of the following format:

Table 81: 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:

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

Table 82: 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:

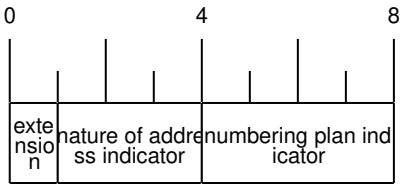



Figure 32: ToN/NPI header coding (as per 3GPP TS 129.002, MSB first)

Please note that unlike both Section 14.7.19 and Section 14.7.20, where the value part is encoded as LV (i.e. contains an additional length), an identity in both Section 14.8.4 / Section 14.8.5 IEs shall not contain the redundant length octet.

#### 14.8.7 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.

#### 14.8.8 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 14.8.8 is used to carry the cause value 'as-is'.

#### 14.8.9 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.

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

#### 14.8.10 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 83: SM Alert Reason values

| Type | Description |
|---|---|
| 0x01 | MS present |
| 0x02 | Memory Available |

# 15 Counters

These counters and their description based on OsmoSGSN 1.4.0.31-05fe (OsmoSGSN).

## 15.1 Rate Counters

Table 84: bssgp:bss_ctx - BSSGP Peer Statistics

| Name | Reference | Description |
|---|---|---|
| packets:in | [?] | Packets at BSSGP Level ( In) |
| packets:out | [?] | Packets at BSSGP Level (Out) |
| bytes:in | [?] | Bytes at BSSGP Level ( In) |
| bytes:out | [?] | Bytes at BSSGP Level (Out) |
| blocked | [?] | BVC Blocking count |
| discarded | [?] | BVC LLC Discarded count |
| status | [?] | BVC Status count |

Table 85: sgsn - SGSN Overall Statistics

| Name | Reference | Description |
|---|---|---|
| llc:dl_bytes | [?] | Count sent LLC bytes before giving it to the bssgp layer |
| llc:ul_bytes | [?] | Count successful received LLC bytes (encrypt & fcs correct) |
| llc:dl_packets | [?] | Count successful sent LLC packets before giving it to the bssgp layer |
| llc:ul_packets | [?] | Count successful received LLC packets (encrypt & fcs correct) |
| gprs:attach_requested | [?] | Received attach requests |
| gprs:attach_accepted | [?] | Sent attach accepts |
| gprs:attach_rejected | [?] | Sent attach rejects |
| gprs:detach_requested | [?] | Received detach requests |
| gprs:detach_acked | [?] | Sent detach acks |
| gprs:routing_area_requested | [?] | Received routing area requests |
| gprs:routing_area_requested | [?] | Sent routing area acks |

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

Table 85: (continued)

| Name | Reference | Description |
|---|---|---|
| gprs:routing_area_requested | [?] | Sent routing area rejects |
| pdp:activate_requested | [?] | Received activate requests |
| pdp:activate_rejected | [?] | Sent activate rejects |
| pdp:activate_accepted | [?] | Sent activate accepts |
| pdp:request_activated | [?] | unused |
| pdp:request_activate_rejected | [?] | unused |
| pdp:modify_requested | [?] | unused |
| pdp:modify_accepted | [?] | unused |
| pdp:dl_deactivate_requested | [?] | Sent deactivate requests |
| pdp:dl_deactivate_accepted | [?] | Sent deactivate accepted |
| pdp:ul_deactivate_requested | [?] | Received deactivate requests |
| pdp:ul_deactivate_accepted | [?] | Received deactivate accepts |

Table 86: ns:nsvc - NSVC Peer Statistics

| Name | Reference | Description |
|---|---|---|
| packets:in | [?] | Packets at NS Level ( In) |
| packets:out | [?] | Packets at NS Level (Out) |
| bytes:in | [?] | Bytes at NS Level ( In) |
| bytes:out | [?] | Bytes at NS Level (Out) |
| blocked | [?] | NS-VC Block count |
| dead | [?] | NS-VC gone dead count |
| replaced | [?] | NS-VC replaced other count |
| nsei-chg | [?] | NS-VC changed NSEI count |
| inv-nsvci | [?] | NS-VCI was invalid count |
| inv-nsei | [?] | NSEI was invalid count |
| lost:alive | [?] | ALIVE ACK missing count |
| lost:reset | [?] | RESET ACK missing count |

# 16 Osmo Stat Items

NSVC Peer Statistics .ns.nsvc - NSVC Peer Statistics

| Name | Reference | Description | Unit |
|---|---|---|---|
| alive.delay | [?] | ALIVE response time | ms |

# 17 Osmo Counters

# 18 Glossary

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**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

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

**BVCI**
BSSGP Virtual Circuit Identifier

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**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

**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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**ETSI**
European Telecommunications Standardization Institute

**FPGA**
Field Programmable Gate Array; programmable digital logic hardware

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

**GERAN**
GPRS/EDGE Radio Access Network

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

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

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

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

**Gp**
Gp interface between SGSN and GGSN; uses GTP protocol

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

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

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

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

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

**GT**
Global Title; an address in SCCP

**GTP**
GPRS Tunnel Protocol; used between SGSN and GGSN

**HLR**
Home Location Register; central subscriber database of a GSM network

**HNB-GW**
Home NodeB Gateway. Entity between femtocells (Home NodeB) and CN in 3G/UMTS.

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

**IE**
Information Element

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**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

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**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

**OML**
Operation & Maintenance Link (ETSI/*3GPP TS 52.021* [3gpp-ts-52-021])

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**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

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

Copyright © 2013-2024 sysmocom - s.f.m.c. GmbH 

**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 © 2013-2024 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 © 2013-2024 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 88: 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 

Table 88: (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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 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 © 2013-2024 sysmocom - s.f.m.c. GmbH 