sysmocom

sysmocom - s.f.m.c. GmbH

OsmoSGSN User Manual

by Harald Welte

The Asciidoc source code of this manual can be found at http://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

Contents

1 Foreword

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

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

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

`bs11-abis` quickly turned into `bsc-hack`, then *OpenBSC* and into what is today known as 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 quick also commercial interest, contribution and adoption. This added 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.

It has been a most exciting ride during the last seven years. I wouldn't want to miss it under any circumstances.

— Harald Welte, Osmocom.org and OpenBSC founder, January 2016.

1.1 Acknowledgements

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

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

May the source be with you!

— Harald Welte, Osmocom.org and OpenBSC founder, January 2016.

1.2 Endorsements

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

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

2 Preface

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

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

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

2.1 FOSS lives by contribution!

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

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

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

We're looking forward to receiving your contributions.

2.2 Osmocom and sysmocom

Some of the founders of the Osmocom project have established sysmocom as a company to provide products and services related to Osmocom.

sysmocom and its staff are the by far the largest developers and contributors 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 requires participation in the FOSS projects any commercial relationship with sysmocom as a company.

2.3 Corrections

We have prepared this manual in the hope 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, mistakes 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 operates in licensed spectrum, please always double-check that you have all required licenses and that you do not transmit on any ARFCN that is not explicitly allocated to you by the applicable regulatory authority in your country.

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

2.4.2 Software License

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

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

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

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

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

2.4.3 Trademarks

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

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

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

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

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

2.4.4 Liability

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

2.4.5 Documentation License

Please see Appendix C for further information.

3 Introduction

3.1 Required Skills

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

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

If you do not share an existing background in GSM network architecture, 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 through to core network configuration/administration.

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

Some of the useful skills we recommend are:

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

3.2 Getting assistance

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

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

4 Overview

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.

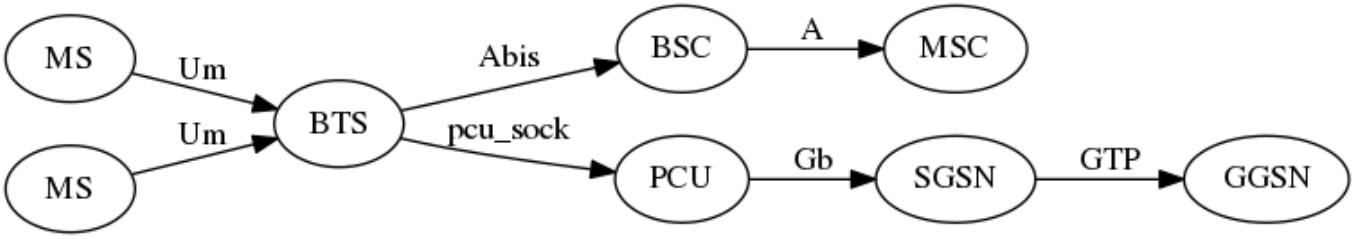


Figure 1: GPRS network architecture with PCU in BTS

4.2 Software Components

OsmoNITB 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.

4.2.2 GTP Implementation

OsmoSGSN uses the libgtp implementation originating from OpenGGSN. 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.

Furthermore, it does not support IP header nor payload compression at this point. Addition of those features is subject to customer demand or user/customer contributions.

The LLC implementation does support LLC encryption. However, as no HLR access is implemented yet, there is no way to enable/configure per-subscriber specific keys.

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.

Currently, all PDP contexts are routed to the same GGSN, irrespective of the APN used/configured in the MS. This is sufficient (and actually desirable) for small autonomous networks, but of course not suitable for real networks in roaming scenarios. Please contact sysmocom in case you require additional features such as DNS-based APN resolving.

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 LLC encryption support
- No interface to the OsmoNITB HLR
- No paging coordination between SGSN and MSC
- No SMS over Ps support
- No IuPS interface for 3G (in progress)
- No IP header compression
- No payload compression

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*]

5.2 OPTIONS

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

-V, --version
Print the compile-time version number of the OsmoBTS 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 11, the variables common to all programs using it are described in Section 11.2. Here we describe variables specific to OsmoSGSN.

Table 1: 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 interaction with Osmocom software is typically performed via an interactive command-line interface called the *VTY*.

The Osmocom VTY is used to

- explore the current status of the system, including its configuration parameters but also run-time state and statistics
- review the currently active (running) configuration
- perform interactive changes to the configuration
- 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.

This chapter explains the most common nodes nodes and the commands that are available within the node.

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 2: VTY Parameter Patterns

Pattern	Example	Explanation
`A.B.C.D`	`127.0.0.1`	An IPv4 address

Table 2: (continued)

Pattern	Example	Explanation
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

7.1 Accessing the VTY

The VTY of a given Osmocom program is implemented as a telnet server, listening to a specific TCP port. For `osmo-nitb`, this port is `4242`.

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
The *VIEW* node is the node you automatically enter when you connect to a VTY. 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 as soon as you enter 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 when you enter the `configure terminal` command from the *VIEW* node. The config node is used to change the run-time configuration parameters of teh 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 Osmcoom GSM/GPRS software, thus this chapter is present in all the relevant manuals. The detailed examples below assume you are executing them on the OsmoNITB VTY. They will work in similar fashion on the other VTY, too - but of course the output will be different for each program.

7.3.1 The question-mark (?) command

If you type a single `?` at the prompt, the VTY will display you 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 OsmoNITB prompt

```
OpenBSC> 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 log message to this terminal
  sms          SMS related commands
  subscriber   Operations on a Subscriber
```

❶ press `?` here at the prompt, the character will not be printed

If you have already entered a partial command, `?` will help you to review possible options of how to continue your command. Let's say you remember that `show` is used to investigate the system status. But you don't know exactly what the object was called that you'd like to show: You simply press `?` after typing `show` and you will see the following choice:

Example: Typing ? after a partial command

```
OpenBSC> show ❶
  version        Displays program version
  online-help    Online help
  history        Display the session command history
  network        Display information about a GSM NETWORK
  bts            Display information about a BTS
  trx            Display information about a TRX
  timeslot       Display information about a TS
  lchan          Display information about a logical channel
  paging         Display information about paging requests of a BTS
  paging-group   Display the paging group
  logging        Show current logging configuration
  alarms         Show current logging configuration
  stats          Show statistical values
  e1_driver      Display information about available E1 drivers
  e1_line        Display information about a E1 line
  e1_timeslot    Display information about a E1 timeslot
  subscriber     Operations on a Subscriber
  statistics     Display network statistics
  sms-queue      Display SMSqueue statistics
  smpp           SMPP Interface
```


❶ press `?` after the `show` command, the character will not be printed

Now you decide you want to have a look at the `network` object, so you type network and press `?` again:

Example: Typing ? after show network

```
OpenBSC> show network
  <cr>
```

By presenting `<cr>` as the only option, the VTY tells you that your command is complete and does not support any additional arguments.

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 choice of possible continuations, or complete the command if there's only one alternative.

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

```
OpenBSC> s❶
show       sms        subscriber
```

❶ press `<tab>` here.

At this point you then have to decide how to continue typing your command. Let's assume you choose `show`, and then press `<tab>` again:

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

```
OpenBSC> show ❶
version    online-help history    network    bts        trx
timeslot   lchan      paging     paging-group logging    alarms
stats      e1_driver  e1_line    e1_timeslot subscriber statistics
sms-queue  smpp
```

❶ press `<tab>` here.

7.3.3 The `list` command

The `list` command will give you a full list of all commands available at this node:

Example: Typing list at start of OsmoNITB VIEW node prompt

```
OpenBSC> list
  show version
  show online-help
  list
  exit
  help
  enable
  terminal length <0-512>
  terminal no length
  who
  show history
  show network
  show bts [<0-255>]
  show trx [<0-255>] [<0-255>]
  show timeslot [<0-255>] [<0-255>] [<0-7>]
  show lchan [<0-255>] [<0-255>] [<0-7>] [lchan_nr]
```



```
  show lchan summary [<0-255>] [<0-255>] [<0-7>] [lchan_nr]
  show paging [<0-255>]
  show paging-group <0-255> IMSI
  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 set-log-mask MASK
  logging level (all|rll|cc|mm|rr|rsl|nm|mncc|pag|meas|sccp|msc|mgcp|ho|db|ref|gprs|ns| ↩
      bssgp|llc|sndcp|nat|ctrl|smpp|filter|lglobal|llapd|linp|lmux|lmi|lmib|lsms|lctrl|lgtp| ↩
      lstats) (debug|info|notice|error|fatal)
  show logging vty
  show alarms
  show stats
  show stats level (global|peer|subscriber)
  show e1_driver
  show e1_line [line_nr] [stats]
  show e1_timeslot [line_nr] [ts_nr]
  show subscriber (extension|imsi|tmsi|id) ID
  show subscriber cache
  sms send pending
  subscriber create imsi ID
  subscriber (extension|imsi|tmsi|id) ID sms sender (extension|imsi|tmsi|id) SENDER_ID send ↩
       .LINE
  subscriber (extension|imsi|tmsi|id) ID silent-sms sender (extension|imsi|tmsi|id)  ↩
      SENDER_ID send .LINE
  subscriber (extension|imsi|tmsi|id) ID silent-call start (any|tch/f|tch/any|sdcch)
  subscriber (extension|imsi|tmsi|id) ID silent-call stop
  subscriber (extension|imsi|tmsi|id) ID ussd-notify (0|1|2) .TEXT
  subscriber (extension|imsi|tmsi|id) ID update
  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, and the current node you're at. Compare the above example of the OsmoNITB *VIEW* node with the result from the OsmoNITB *TRX* config node:

Example: Typing list at start of OsmoNITB TRX config node prompt

```
OpenBSC(config-net-bts-trx)# list
  help
  list
  write terminal
  write file
  write memory
  write
  show running-config
  exit
  end
  arfcn <0-1023>
  description .TEXT
  no description
  nominal power <0-100>
```



```
max_power_red <0-100>
rsl e1 line E1_LINE timeslot <1-31> sub-slot (0|1|2|3|full)
rsl e1 tei <0-63>
rf_locked (0|1)
timeslot <0-7>
```

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 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 your VTY session. 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 OpenBSC, there are categories for the protocol layers `rsl`, `rr`, `mm`, `cc` and many others. To get a a list of categories interactively on the vty, type: `logging level ?`

For each of those categories, 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.

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 OpenBSC, to set the log level of the Mobility Management category to info, you can use the following command: `log level mm info`.

Equally, 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. 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`

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

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.

8.2 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:

```
OpenBSC> enable
OpenBSC# configure terminal
OpenBSC(config)# log file /path/to/my/file
OpenBSC(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 currently does not provide file close-and-reopen support by SIGHUP, as used by popular log file rotating solutions. Please contact the Osmocom developers if you require this feature to be implemented.

8.3 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:

```
OpenBSC> enable
OpenBSC# configure terminal
OpenBSC(config)# log syslog daemon
OpenBSC(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.

8.4 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:

```
OpenBSC> enable
OpenBSC# configure terminal
OpenBSC(config)# log stderr
OpenBSC(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 all 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

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 a 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
```

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 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>
```

❶ *acl-only* is selected as authorization policy

❷ Saves current changes to cofiguration to make this policy persistent

Example: Access control list:

```
sgsn
 auth-policy acl-only ❶
 imsi-acl add 001010000000003
 imsi-acl add 001010000000002
 imsi-acl add 001010000000001
 imsi-acl add 901700000000068 ❷
```

❶ Set the authorization policy

❷ Add as many subscribers as required

9.3 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 9.2

9.3.1 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 MILEAGE 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 ❶
OsmoSGSN(config-sgsn)# gsup remote-port 10000 ❷
OsmoSGSN(config-sgsn)# gsup oap-k 000102030405060708090a0b0c0d0e0f ❸
OsmoSGSN(config-sgsn)# gsup oap-opc 101112131415161718191a1b1c1d1e1f ❹
```

❶ Configure the IP address of the (remote) HLR or HLR-GW

❷ Configure the TCP port of the (remote) HLR or HLR-GW

❸ Specify the OAP shared key

❹ Specify the OAP shared OPC

9.4 CDR configuration

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

Example: CDR 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.

Table 3: 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 4
pdp	
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

Table 4: 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

9.5 User traffic compression

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

9.5.1 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
```

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)

9.5.2 Data compression

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

compression rfc1144 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
```

10 Gb interface using libosmogb

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 project, including OsmoSGSN, OsmoGbProxy and OsmoPCU.

This section describes the configuration that libosmogb exposes via the VTY.

10.1 Gb interface configuration

10.1.1 NS-over-UDP configuration

The GPRS-NS protocol can be encapsulated in UDP/IP. This is the default encapsulation for IP based GPRS systems.

Example: GPRS NS-over-UDP configuration

```
OsmoSGSN(config-ns)# encapsulation udp local-ip 127.0.0.1 ❶
OsmoSGSN(config-ns)# encapsulation udp local-port 23000 ❷
```

The example above configures a libosmogb based application to listen for incoming connections from PCUs on the specified address and port.

❶ Set the local side IP address for NS-over-UDP

❷ Set the local side UDP port number for NS-over-UDP. 23000 is the default

10.1.2 NS-over-FR-GRE configuration

The GPRS-NS protocol can alternatively be encapsulated over Frame Relay (FR). Traditionally this is communicated over SDH/PDH media, which we don't support. However, we can encapsulate the FR in GRE, and then that in IP.

The resulting NS-FR-GRE-IP stack can be converted by an off-the-shelf router with FR and IP support.

Example: GPRS NS-over-FR-GRE configuration

```
OsmoSGSN(config-ns)# encapsulation framerelay-gre enabled 1 ❶
OsmoSGSN(config-ns)# encapsulation framerelay-gre local-ip 127.0.0.1 ❷
```

❶ Enable FR-GRE encapsulation

❷ Set the local side IP address for NS-over-FR-GRE

10.1.3 NS Timer configuration

The NS protocol features a number of configurable timers.

Table 5: 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

10.2 Examining Gb interface status

There are several commands that can help to inspect and analyze the currently running system status with respect to the Gb interfaces.

Example: Inspecting NS state

```
OsmoSGSN> show ns
Encapsulation NS-UDP-IP     Local IP: 127.0.0.1, UDP Port: 23000
Encapsulation NS-FR-GRE-IP  Local IP: 0.0.0.0
```

Example: Inspecting NS statistics

```
OsmoSGSN> show ns stats
Encapsulation NS-UDP-IP     Local IP: 10.9.1.198, UDP Port: 23000
Encapsulation NS-FR-GRE-IP  Local IP: 0.0.0.0
NSEI  101, NS-VC 101, Remote: BSS, ALIVE UNBLOCKED, UDP 10.9.1.119:23000
 NSVC Peer Statistics:
  Packets at NS Level  ( In):     1024 (2/s 123/m 911/h 0/d)
  Packets at NS Level  (Out):     1034 (0/s 151/m 894/h 0/d)
  Bytes at NS Level    ( In):   296638 (1066/s 22222/m 274244/h 0/d)
  Bytes at NS Level    (Out):   139788 (0/s 48225/m 91710/h 0/d)
  NS-VC Block count          :        0 (0/s 0/m 0/h 0/d)
  NS-VC gone dead count      :        0 (0/s 0/m 0/h 0/d)
  NS-VC replaced other count:        0 (0/s 0/m 0/h 0/d)
  NS-VC changed NSEI count   :        0 (0/s 0/m 0/h 0/d)
```



```
  NS-VCI was invalid count  :        0 (0/s 0/m 0/h 0/d)
  NSEI was invalid count    :        0 (0/s 0/m 0/h 0/d)
  ALIVE ACK missing count   :        0 (0/s 0/m 0/h 0/d)
  RESET ACK missing count   :        0 (0/s 0/m 0/h 0/d)
 NSVC Peer Statistics:
  ALIVE reponse time        :        0 ms
```

Example: Inspecting BSSGP state

```
OsmoSGSN> show bssgp
NSEI   101, BVCI     2, RA-ID: 1-2-1-0, CID: 0, STATE: UNBLOCKED
NSEI   101, BVCI     0, RA-ID: 0-0-0-0, CID: 0, STATE: UNBLOCKED
```

FIXME: show nse

10.3 FIXME

10.3.1 Blocking / Unblocking / Resetting NS Virtual Connections

The user can manually perform operations on individual NSVCs:

- blocking a NSVC
- unblocking a NSVC
- resetting a NSVC

The VTY command used for this is the `nsvc (nsei|nsvci) <0-65535> (block|unblock|reset)` command available from the ENABLE node.

10.4 Gb interface logging filters

There are some Gb-interface specific filters for the libosmocore logging subsystem, which can help to reduce the logged output to messages pertaining to a certain NS or BSSGP connection only.

Example: enabling a log filter for a given NSEI

```
OsmoSGSN> logging filter nsvc nsei 23
```

Example: enabling a log filter for a given NSVCI

```
OsmoSGSN> logging filter nsvc nsvci 23
```

11 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.

11.1 Control Interface Protocol

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

The protocol for the control interface is wrapped inside the IPA multiplex header with the stream identifier set to IPAC_PROTO_OSMO (0xEE).

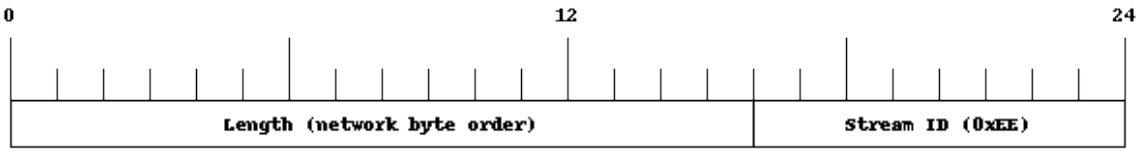


Figure 2: IPA header for control protocol

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

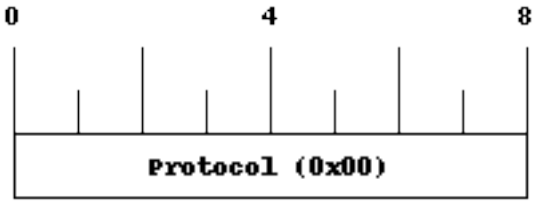


Figure 3: IPA extension header for control protocol

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. `0` is not allowed. It will be echoed back in any response to a particular request.

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

<val>
The value of the variable / field

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

11.1.1 GET operation

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

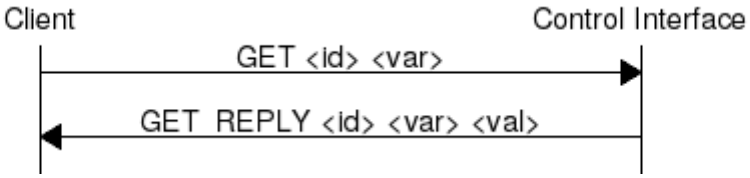


Figure 4: Control Interface GET operation (successful outcome)

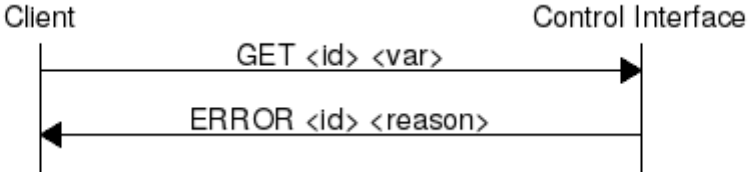


Figure 5: Control Interface GET operation (unsuccessful outcome)

11.1.2 SET operation

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

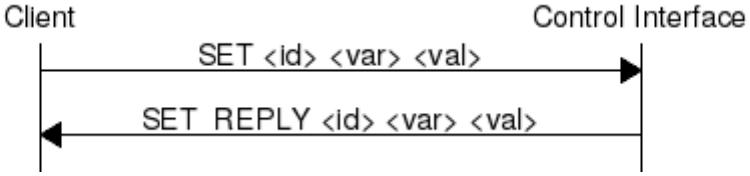


Figure 6: Control Interface SET operation (successful outcome)

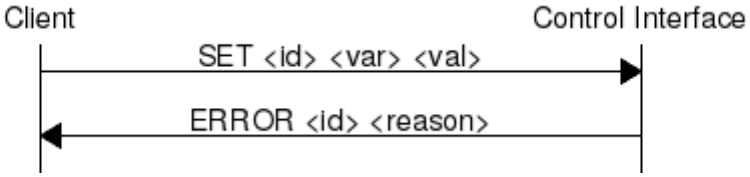


Figure 7: Control Interface SET operation (unsuccessful outcome)

11.1.3 TRAP operation

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

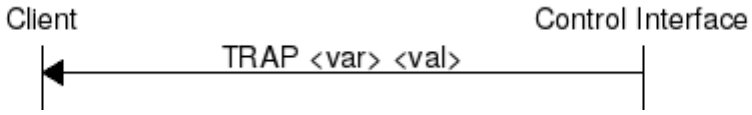


Figure 8: Control Interface TRAP operation

11.2 Common variables

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

Table 6: Variables available over control interface

Name	Access	Value	Comment
counter.*	RO		Get counter value.
rate_ctr.*	RO		Get rate counter value.

Those read-only variables allow to get value of arbitrary counter or rate counter using its name e. g. "counter.net.sms.submitted" or "rate_ctr.per_hour.nat.bsc.sccp.conn". Of course for that to work the program in question have to register corresponding counter names using libosmocore functions. Note the difference between counter and rate_ctr access format: in case of rate_ctr the counter 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.

11.3 Control Interface python example: `bsc_control.py`

In the `openbsc.git` repository, there is an example python script called `openbsc/contrib/bsc_control.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.

11.3.1 Setting a value

Example: Use bsc_control.py to set the short network name of OsmoNITB

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

11.3.2 Getting a value

Example: Use bsc_control.py to get the mnc of OsmoNITB

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


11.3.3 Listening for traps

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

Example: Using bsc_control.py to listen for traps:

```
$ ./bsc_control.py -d localhost -m
❶
```

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

12 Osmocom Authentication Protocol (OAP)

12.1 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.

12.2 Connection

The protocol expects that a reliable, ordered, packet boundaries preserving connection is used (e.g. IPA over TCP).

12.3 Using IPA

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

12.4 Procedures

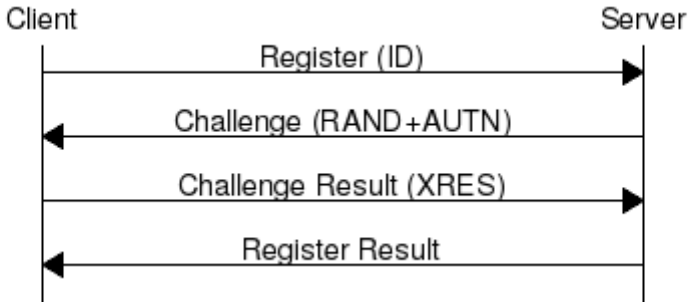


Figure 9: Ideal communication sequence

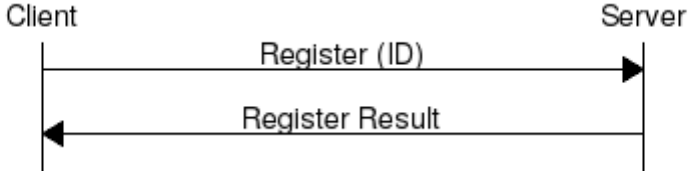


Figure 10: Variation "test setup"

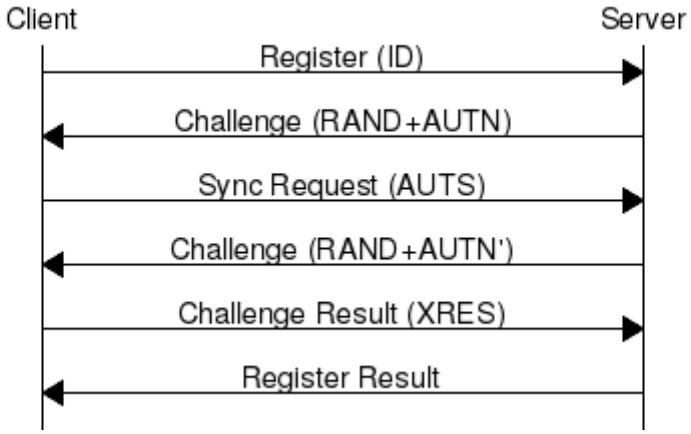


Figure 11: Variation "invalid sequence nr":

12.4.1 Register

The client sends a REGISTER_REQ message containing an identifier number.

12.4.2 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.

12.4.3 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 secet. 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.

12.4.4 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.

12.4.5 Sync Result

If the server has received a valid Sync Request, it shall answer by directly sending another Challenge (see Section 12.4.2). If an invalid Sync Request is received, the server shall reply with a REGISTER_ERR message.

12.4.6 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.

12.5 Message Format

Every message is based on the following message format

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1

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

12.5.1 Register Request

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1
30	Client ID	Section 12.6.3	M	TLV	4

12.5.2 Register Error

Direction: Server → Client

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1
02	Cause	GMM Cause, TS 04.08: 10.5.5.14	M	TLV	3

12.5.3 Register Result

Direction: Server → Client

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1

12.5.4 Challenge

Direction: Server → Client

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1
20	RAND	octet string (16)	TLV	18	23

12.5.5 Challenge Error

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1
02	Cause	GMM Cause, TS 04.08: 10.5.5.14	M	TLV	3

12.5.6 Challenge Result

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1

12.5.7 Sync Request

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 12.6.1	M	V	1

12.5.8 Sync Error

Not used.

12.5.9 Sync Result

Not used.

12.6 Information Elements

12.6.1 Message Type

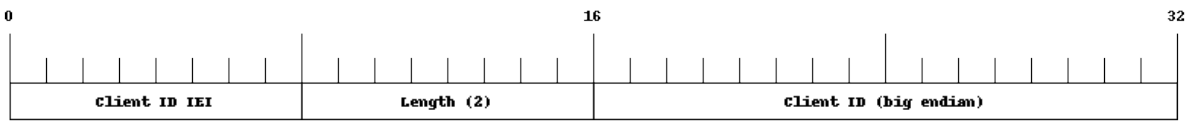
0x04	Register Requst
0x05	Register Error
0x06	Register Result
0x08	Challenge Request
0x09	Challenge Error
0x0a	Challenge Result
0x0c	Sync Request
0x0d	Sync Error (not used)
0x0e	Sync Result (not used)

12.6.2 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

12.6.3 Client ID



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

13 GPRS Subscriber Update Protocol

13.1 General

This chapter describes the remote protocol that is used by the SGSN to update and manage the local subscriber list. Functionally, it resembles the interface between the SGSN 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 stck of MTP2/MTP3/SCCP/TCAP, or any of the SIGTRAN alternatvives.

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

The GSUP protocol and the messages are designed after the corresponding MAP messages (see 3GPP TS 09.02) with the following main differences:

- The encoding uses TLV structures instead of ASN.1 BER
- Segmentation is not used, i.e. we rely on the fact that the underlying transport protocol can transport signalling messages of any size.

13.2 Connection

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

13.3 Using IPA

By default, the following identifiers should be used:

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

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

13.4 Procedures

13.4.1 Authentication management

The SGSN 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 replaces all tuples that are assigned to the subscriber. If the message doesn't contain any tuple the SGSN may reject the Attach Request. (see 3GPP TS 09.02, 25.5.6)

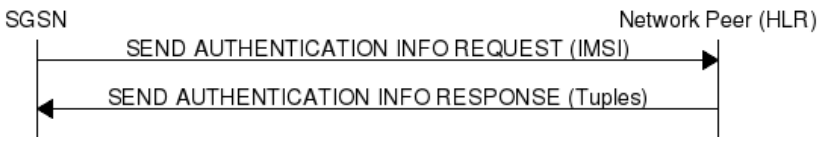


Figure 12: Send Authentication Info (Normal Case)

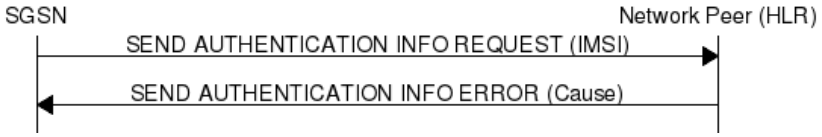


Figure 13: Send Authentication Info (Erroneous Case)

13.4.2 Reporting of Authentication Failure

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

Figure 14: Authentication Failure Report (Normal Case)

13.4.3 Location Updating

The SGSN 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. 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 clears existing PDP information fields in the subscriber record first. (see 3GPP TS 09.02, 19.1.1.8)

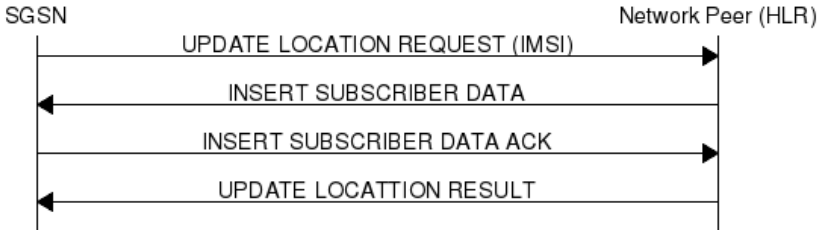


Figure 15: Update Location (Normal Case)

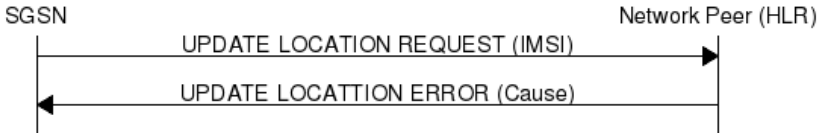


Figure 16: Update Location (Error Case)

13.4.4 Location Cancellation

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

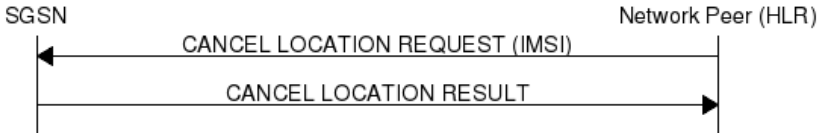


Figure 17: Cancel Location (Normal Case)

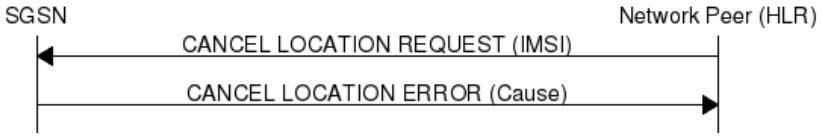


Figure 18: Cancel Location (Error Case)

13.4.5 Purge MS

Using the Purge MS procedure, the SGSN can request purging of MS related state from a previous SGSN during an inter-SGSN location update.

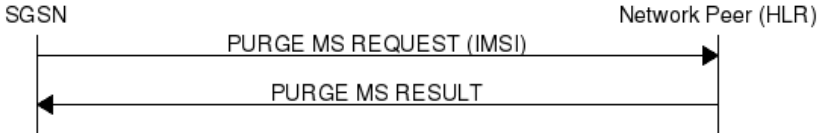


Figure 19: Purge MS (Normal Case)

13.4.6 Delete Subscriber Data

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

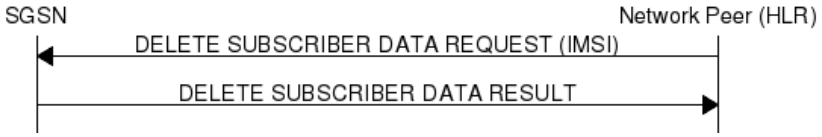


Figure 20: Delete Subscriber Data (Normal Case)

13.5 Message Format

13.5.1 General

Every message is based on the following message format

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	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.

13.5.2 Send Authentication Info Request

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
28	CN Domain	Section 13.6.15	O	TLV	3
26	AUTS	Section 13.6.13	C	TLV	18
20	RAND	Section 13.6.7	C	TLV	18

The conditional *AUTS* and *RAND* IEs are both present in case the SIM (via UE) requests an UMTS AKA re-synchronization procedure. Eiter both optional IEs are present, or none of them.

13.5.3 Send Authentication Info Error

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
02	Cause	Section 13.6.25	M	TLV	3

13.5.4 Send Authentication Info Response

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
03	Auth Tuple	Section 13.6.6	0-5	TLV	36

13.5.5 Authentication Failure Report

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
28	CN Domain	Section 13.6.15	O	TLV	3

13.5.6 Update Location Request

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10

IEI	IE	Type	Presence	Format	Length
28	CN Domain	Section 13.6.15	O	TLV	3

13.5.7 Update Location Error

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
02	Cause	Section 13.6.25	M	TLV	3

13.5.8 Update Location Result

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
08	MSISDN	Section 13.6.20	O	TLV	0-9
09	HLR Number	Section 13.6.24	O	TLV	0-9
04	PDP info complete	Section 13.6.18	O	TLV	2
05	PDP info	Section 13.6.3	1-10	TLV	

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

13.5.9 Location Cancellation Request

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
28	CN Domain	Section 13.6.15	O	TLV	3
06	Cancellation type	Section 13.6.16	O	TLV	3

13.5.10 Location Cancellation Result

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
28	CN Domain	Section 13.6.15	O	TLV	3

13.5.11 Purge MS Request

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10

IEI	IE	Type	Presence	Format	Length
28	CN Domain	Section 13.6.15	O	TLV	3
09	HLR Number	Section 13.6.24	M	TLV	0-9

13.5.12 Purge MS Error

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
02	Cause	Section 13.6.25	M	TLV	3

13.5.13 Purge MS Result

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
07	Freeze P-TMSI	Section 13.6.18	M	TLV	2

13.5.14 Insert Subscriber Data Request

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
28	CN Domain	Section 13.6.15	O	TLV	3
08	MSISDN	Section 13.6.20	O	TLV	0-9
09	HLR Number	Section 13.6.24	O	TLV	0-9
04	PDP info complete	Section 13.6.18	M	TLV	2
05	PDP info	Section 13.6.3	0-10	TLV	
14	PDP-Charging Characteristics	Section 13.6.23	O	TLV	4

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

13.5.15 Insert Subscriber Data Error

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
02	Cause	Section 13.6.25	M	TLV	3

13.5.16 Insert Subscriber Data Result

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10

13.5.17 Delete Subscriber Data Request

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
28	CN Domain	Section 13.6.15	O	TLV	3
10	PDP context id	Section 13.6.3 (no conditional IE)	0-10	TLV	

13.5.18 Delete Subscriber Data Error

Direction: SGSN ⇒ Network peer

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10
02	Cause	Section 13.6.25	M	TLV	3

13.5.19 Delete Subscriber Data Result

Direction: Network peer ⇒ SGSN

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 13.6.1	M	V	1
01	IMSI	Section 13.6.19	M	TLV	2-10

13.6 Information Elements

13.6.1 Message Type

Type	Description
0x04	Update Location Request
0x05	Update Location Error
0x06	Update Location Result
0x08	Send Auth Info Request
0x09	Send Auth Info Error
0x0a	Send Auth Info Result
0x0b	Authentication Failure Report
0x0c	Purge MS Request
0x0d	Purge MS Error
0x0e	Purge MS Result
0x10	Insert Subscriber Data Request
0x11	Insert Subscriber Data Error
0x12	Insert Subscriber Data Result
0x14	Delete Subscriber Data Request
0x15	Delete Subscriber Data Error
0x16	Delete Subscriber Data Result

Type	Description
0x1c	Location Cancellation Request
0x1d	Location Cancellation Error
0x1e	Location Cancellation Result

13.6.2 IP Address

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

13.6.3 PDP Info

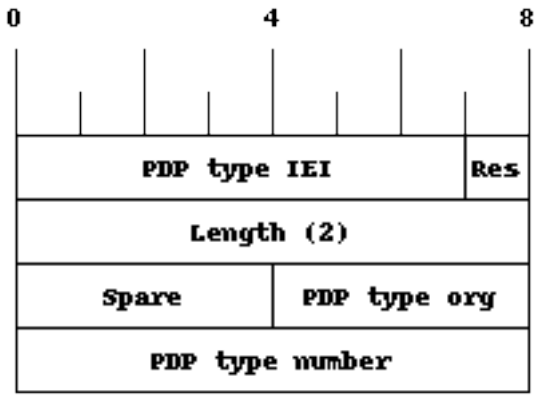
This is a container for information elements describing a single PDP.

IEI	IE	Type	Presence	Format	Length
	PDP Info IEI	Section 13.6.17	M	V	1
	Length of PDP Info IE		M	V	1
10	PDP Context ID	Section 13.6.5	C	TLV	3
11	PDP Type	Section 13.6.4	C	TLV	4
12	Access Point Name	Section 13.6.21	C	TLV	3-102
13	Quality of Service	Section 13.6.22	O	TLV	1-20
14	PDP-Charging Characteristics	Section 13.6.23	O	TLV	4

The conditional IE are mandantory unless mentioned otherwise.

13.6.4 PDP Type

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



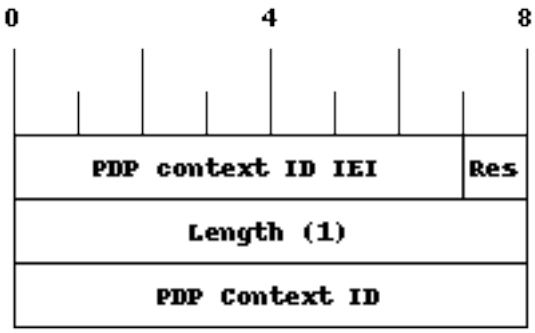
The spare bits are left undefined. While 09.60 defines them as *1 1 1 1*, there are MAP traces where these bits are set to *0 0 0 0*. So the receiver shall ignore these bits.

Examples:

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

13.6.5 PDP Context ID

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



13.6.6 Auth tuple

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

IEI	IE	Type	Presence	Format	Length
	Auth Tuple IEI	Section 13.6.17	M	V	1
	Length of Auth Tuple IE		M	V	1
20	RAND	Section 13.6.7	M	TLV	18
21	SRES	Section 13.6.8	M	TLV	6
22	Kc	Section 13.6.9	M	TLV	10
23	IK	Section 13.6.10	C	TLV	18
24	CK	Section 13.6.11	C	TLV	18
25	AUTN	Section 13.6.12	C	TLV	18
27	RES	Section 13.6.14	C	TLV	2-18

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

13.6.7 RAND

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

13.6.8 SRES

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

13.6.9 Kc

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

13.6.10 IK

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

13.6.11 CK

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

13.6.12 AUTN

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

13.6.13 AUTS

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

13.6.14 RES

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

13.6.15 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 7: CN Domain Number

Type	Description
0x01	PS Domain
0x02	CS Domain

13.6.16 Cancellation Type

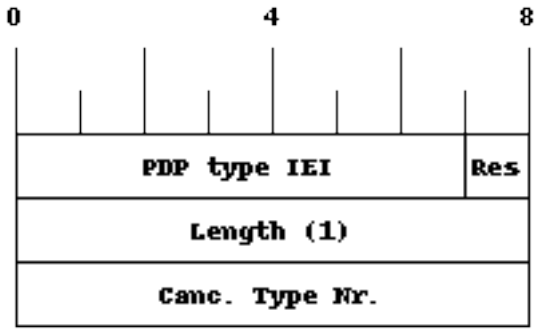


Table 8: Cancellation Type Number

Number	Description
0x00	Update Procedure
0x01	Subscription Withdrawn

13.6.17 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 9: GSUP IE Identifiers

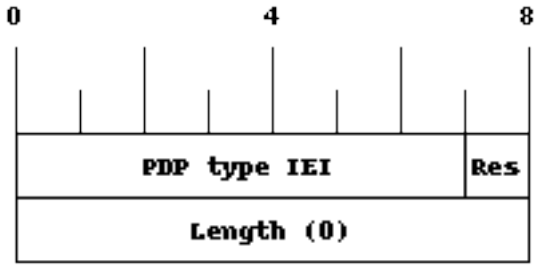
IEI	Info Element	Type / Encoding
0x01	IMSI	Mobile Identity, 3GPP TS 04.08 Ch. 10.5.1.4
0x02	Cause	Section 13.6.25
0x03	Auth Tuple	Section 13.6.6
0x04	PDP Info Compl	Section 13.6.18
0x05	PDP Info	Section 13.6.3
0x06	Cancel Type	Section 13.6.16
0x07	Freeze P-TMSI	Section 13.6.18
0x08	MSISDN	ISDN-AddressString/octet, Section 13.6.20
0x09	HLR Number	Section 13.6.24
0x10	PDP Context ID	Section 13.6.5
0x11	PDP Type	Section 13.6.4
0x12	Access Point Name	Section 13.6.21
0x13	QoS	Section 13.6.22
0x14	PDP-Charging Characteristics	Section 13.6.23
0x20	RAND	Section 13.6.7
0x21	SRES	Section 13.6.8
0x22	Kc	Section 13.6.9
0x23	IK	Section 13.6.10
0x24	CK	Section 13.6.11
0x25	AUTN	Section 13.6.12

Table 9: (continued)

IEI	Info Element	Type / Encoding
0x26	AUTS	Section 13.6.13
0x27	RES	Section 13.6.14
0x28	CN Domain	Section 13.6.15

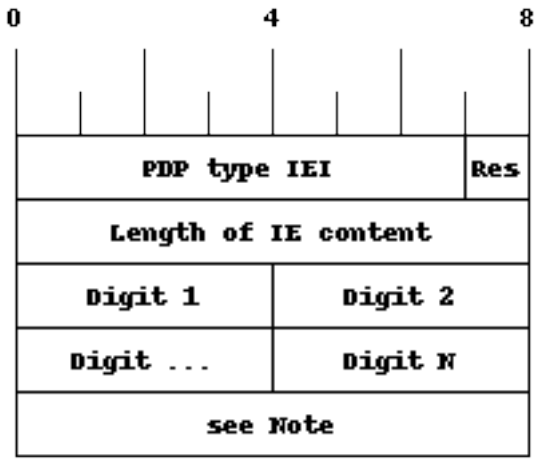
13.6.18 Empty field

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



13.6.19 IMSI

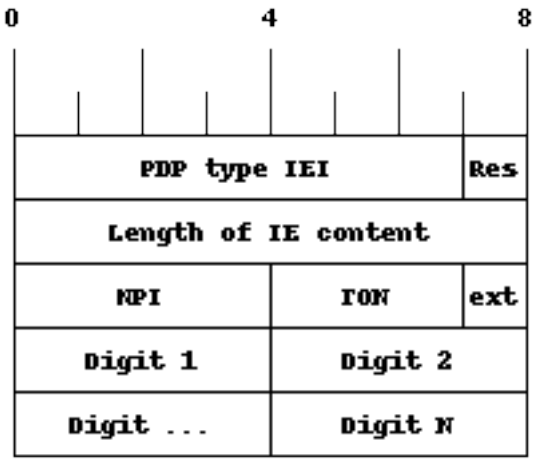
The IMSI is encoded like in octet 4-N of the Called Party BCD Number defined in 3GPP TS 04.08, 10.5.4.7.



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

13.6.20 ISDN-AddressString / MSISDN / Called Party BCD Number

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

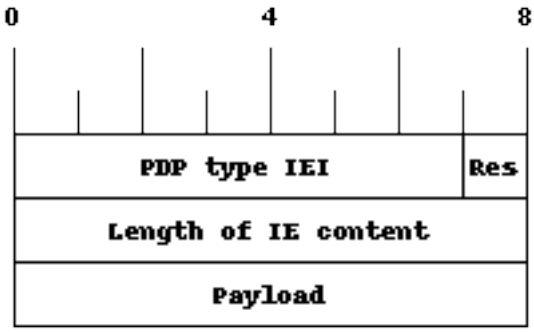


13.6.21 Access Point Name

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

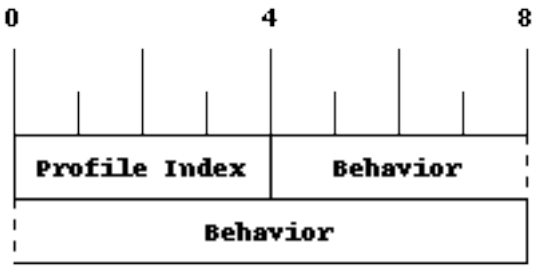
13.6.22 Quality of Service Subscribed Service

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 reset are encoded as octets 3-N of 24.008.



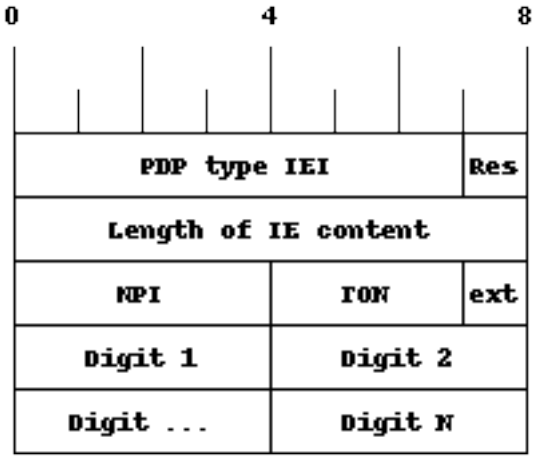
13.6.23 PDP-Charging Characteristics

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 when activating a PDP context.



13.6.24 HLR Number encoded as 3GPP TS 09.02 ISDN-AddressString

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



13.6.25 Cause

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

14 Glossary

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

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

3GPP
3rd Generation Partnership Project

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

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

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

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

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

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

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

AGPL
GNU Affero General Public License, a copyleft-style Free Software License

ARFCN
Absolute Radio Frequency Channel Number; specifies a tuple of uplink and downlink frequencies

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

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

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

BTS
Base Transceiver Station

BSC
Base Station Controller

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

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

BVCI
BSSGP Virtual Circuit Identifier

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

CC
Call Control; Part of the GSM Layer 3 Protocol

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

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

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

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

dB
deci-Bel; relative logarithmic unit

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

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

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

DSP
Digital Signal Processor

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

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

ETSI
European Telecommunications Standardization Institute

FPGA
Field Programmable Gate Array; programmable digital logic hardware

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

GERAN
GPRS/EDGE Radio Access Network

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

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

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

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

Gp
Gp interface between SGSN and GGSN; uses GTP protocol

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

GTP
GPRS Tunnel Protocol; used between SGSN and GGSN

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

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 identifier for the mobile phone

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

IP
Internet Protocol (*IETF RFC 791* [?])

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

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

MCC
Mobile Country Code; unique identifier of a country, e.g. 262 for Germany

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

MGW
Media Gateway

MM
Mobility Management; part of the GSM Layer 3 Protocol

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

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

MS
Mobile Station; a mobile phone / GSM Modem

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

MSISDN
Mobile Subscriber ISDN Number; telephone number of the subscriber

MVNO
Mobile Virtual Network Operator; Operator without physical radio network

NCC
Network Color Code; assigned by national regulator

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

NSEI
NS Entity Identifier

NVCI
NS Virtual Circuit Identifier

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

NS
Network Service; protocol on Gb interface (*3GPP TS 48.016* [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])

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

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

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

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

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

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

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

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

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

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

RF
Radio Frequency

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

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

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

RR
Radio Resources; Part of the GSM Layer 3 Protocol

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

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

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

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

SDK
Software Development Kit

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

SSH
Secure Shell; *IETF RFC 4250* [ietf-rfc4251] to 4254

syslog
System logging service of UNIX-like operating systems

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

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

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

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

TRX
Transceiver; element of a BTS serving a single carrier

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

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

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 10: TCP/UDP port numbers

L4 Protocol	Port Number	Purpose	Software
UDP	2427	MGCP GW	osmo-bsc_mgcp
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	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
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
TCP	4255	Control Interface	osmo-msc
TCP	4256	telnet (VTY)	osmo-sip-connector
TCP	4257	Control Interface	ggsn (OpenGGSN)
TCP	4258	telnet (VTY)	osmo-hlr
TCP	4259	Control Interface	osmo-hlr
TCP	4260	telnet (VTY)	ggsn (OpenGGSN)
UDP	4729	GSMTAP	Almost every osmocom project
TCP	5000	A/IP	osmo-bsc, osmo-bsc_nat
UDP	2427	GSMTAP	osmo-pcu, osmo-bts
UDP	23000	GPRS-NS over IP default port	osmo-pcu, osmo-sgsn, osmo-gbproxy

B Bibliography / References

B.0.25.0.1 References

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

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

[3] [vty-ref-osmobts] Osmocom Project: OsmoBTS VTY Reference Manual. http://ftp.osmocom.org/docs/latest/-osmobts-vty-reference.pdf

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

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

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

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

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

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

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

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

[12] [3gpp-ts-23-048] 3GPP TS 23.048: Security mechanisms for the (U)SIM application toolkit; Stage 2 http://www.3gpp.org/DynaReport/23048.htm

[13] [3gpp-ts-24-007] 3GPP TS 24.007: Mobile radio interface signalling layer 3; General Aspects http://www.3gpp.org/DynaReport/24007.htm

[14] [3gpp-ts-24-008] 3GPP TS 24.008: Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. http://www.3gpp.org/dynareport/24008.htm

[15] [3gpp-ts-31-101] 3GPP TS 31.101: UICC-terminal interface; Physical and logical characteristics http://www.3gpp.org/DynaReport/31101.htm

[16] [3gpp-ts-31-102] 3GPP TS 31.102: Characteristics of the Universal Subscriber Identity Module (USIM) application http://www.3gpp.org/DynaReport/31102.htm

[17] [3gpp-ts-31-111] 3GPP TS 31.111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) http://www.3gpp.org/DynaReport/31111.htm

[18] [3gpp-ts-31-115] 3GPP TS 31.115: Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications http://www.3gpp.org/DynaReport/31115.htm

[19] [3gpp-ts-31-116] 3GPP TS 31.116: Remote APDU Structure for (U)SIM Toolkit applications http://www.3gpp.org/DynaReport/31116.htm

[20] [3gpp-ts-35-205] 3GPP TS 35.205: 3G Security; Specification of the MILENAGE algorithm set: General

[21] [3gpp-ts-35-206] 3GPP TS 35.206: 3G Security; Specification of the MILENAGE algorithm set: Algorithm specification http://www.3gpp.org/DynaReport/35206.htm

[22] [3gpp-ts-44-006] 3GPP TS 44.006: Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification http://www.3gpp.org/DynaReport/44006.htm

[23] [3gpp-ts-44-064] 3GPP TS 44.064: Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification http://www.3gpp.org/DynaReport/44064.htm

[24] [3gpp-ts-48-008] 3GPP TS 48.008: Mobile Switching Centre - Base Station system (MSC-BSS) interface; Layer 3 specification http://www.3gpp.org/DynaReport/48008.htm

[25] [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 http://www.3gpp.org/DynaReport/48016.htm

[26] [3gpp-ts-48-018] 3GPP TS 48.018: General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS protocol (BSSGP) http://www.3gpp.org/DynaReport/48018.htm

[27] [3gpp-ts-48-056] 3GPP TS 48.056: Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 specification http://www.3gpp.org/DynaReport/48056.htm

[28] [3gpp-ts-48-058] 3GPP TS 48.058: Base Station Controller - Base Transceiver Station (BSC - BTS) Interface; Layer 3 specification http://www.3gpp.org/DynaReport/48058.htm

[29] [3gpp-ts-51-011] 3GPP TS 51.011: Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface

[30] [3gpp-ts-51-014] 3GPP TS 51.014: Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface http://www.3gpp.org/DynaReport/51014.htm

[31] [3gpp-ts-52-021] 3GPP TS 52.021: Network Management (NM) procedures and messages on the A-bis interface http://www.3gpp.org/DynaReport/52021.htm

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

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

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

[35] [ietf-rfc768] IETF RFC 768: Internet Protocol https://tools.ietf.org/html/rfc791

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

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

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

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

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

[41] [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

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

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

C GNU Free Documentation License

Version 1.3, 3 November 2008

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:

a. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

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

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

d. Preserve all the copyright notices of the Document.

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

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

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

h. Include an unaltered copy of this License.

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

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

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

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

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

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

o. Preserve any Warranty Disclaimers.

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

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

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

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

C.6 COMBINING DOCUMENTS

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

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

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

C.7 COLLECTIONS OF DOCUMENTS

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

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

C.8 AGGREGATION WITH INDEPENDENT WORKS

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

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

C.9 TRANSLATION

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

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

C.10 TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

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

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

C.11 FUTURE REVISIONS OF THIS LICENSE

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

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

C.12 RELICENSING

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

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

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

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

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

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

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

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

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with…Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

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

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

