sysmocom

sysmocom - s.f.m.c. GmbH

Osmo GSM Manuals Shared Content Test

by Oliver Smith

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

HISTORY			
NUMBER	DATE	DESCRIPTION	NAME
1	6th November 2018	Initial	os

Contents

1 Abis/IP Interface

1.1 A-bis Operation & Maintenance Link

The GSM Operation & Maintenance Link (OML) is specified in 3GPP TS 12.21 and is used between a GSM Base-Transceiver-Station (BTS) and a GSM Base-Station-Controller (BSC). The default TCP port for OML is *3002*. The connection will be opened from the BTS to the BSC.

Abis OML is only specified over E1 interfaces. The Abis/IP implementation of OsmoBTS and OsmoBSC extend and/or deviate from the TS 12.21 specification in several ways. Please see the *OsmoBTS Abis Protocol Specification* [osmobts-abis-spec] for more information.

1.2 A-bis Radio Signalling Link

The GSM Radio Signalling Link (RSL) is specified in 3GPP TS 08.58 and is used between a GSM Base-Transceiver-Station and a GSM Base-Station-Controller (BSC). The default TCP port for RSL is *3003*. The connection will be opened from the BTS to BSC after it has been instructed by the BSC.

Abis RSL is only specified over E1 interfaces. The Abis/IP implementation of OsmoBTS and OsmoBSC extend and/or deviate from the TS 08.58 specification in several ways. Please see the *OsmoBTS Abis Protocol Specification* [osmobts-abis-spec] for more information.

1.3 Locate Abis/IP based BTS

We can use a tool called abisip-find to be able to find BTS which is connected in the network. This tool is located in the OsmoBSC project repository under: *./src/ipaccess*

1.3.1 abisip-find

abisip-find is a small command line tool which is used to search and find BTS devices in your network (e.g. sysmoBTS, nanoBTS).

It uses broadcast packets of the UDP variant of the Abis-IP protocol on port 3006, and thus will find any BTS that can be reached by the all-network broadcast address 255.255.255.255

When program is started it will print one line for each BTS it can find.

Example: using abisip-find to find BTS in your network

```
$ ./abisip-find
abisip-find (C) 2009 by Harald Welte
This is FREE SOFTWARE with ABSOLUTELY NO WARRANTY

you might need to specify the outgoing
network interface, e.g. ``abisip-find eth0``
Trying to find ip.access BTS by broadcast UDP...

MAC_Address='24:62:78:01:02:03' IP_Address='192.168.0.171' Serial_Number='123'
Unit_ID='sysmoBTS 1002'

MAC_Address='24:62:78:04:05:06' IP_Address='192.168.0.182' Serial_Number='456'
Unit_ID='sysmoBTS 1002'

MAC Address='00:01:02:03:04:05' IP Address='192.168.100.123' Unit ID='65535/0/0'
Location_1='' Location 2='BTS_NBT131G'  Equipment Version='165a029_55'
Software Version='168a302_v142b13d0' Unit Name='nbts-00-02-95-00-4E-B3'
Serial Number='00123456'

^C
```


You may have to start the program as a root:

```
$ sudo ./abisip-find eth0
```

1.4 Deploying a new nanoBTS

A tool called ipaccess-config can be used to configure a new ip.access nanoBTS.

1.4.1 ipaccess-config

This program is very helpful tool which is used to configure Unit ID and Primarly OML IP. You can find this tool in the OsmoBSC repository under: *./src/ipaccess*

Example: using ipaccess-config to configure Unit ID and Primarly OML IP of nanoBTS

```
$ ./ipaccess-config -u 1801/0/0❶  10.9.1.195❷ -o 10.9.1.154❸

ipaccess-config (C) 2009-2010 by Harald Welte and others
This is FREE SOFTWARE with ABSOLUTELY NO WARRANTY

Trying to connect to ip.access BTS ...
abis_nm.c:316 OC=SITE-MANAGER(00) INST=(ff,ff,ff) STATE CHG:
OP_STATE=Disabled AVAIL=Not installed(07)
abis_nm.c:316 OC=BTS(01) INST=(00,ff,ff) STATE CHG:
OP_STATE=Disabled AVAIL=Not installed(07) ADM=Locked
abis_nm.c:316 OC=BASEBAND-TRANSCEIVER(04) INST=(00,00,ff) STATE CHG:
OP_STATE=Disabled AVAIL=Not installed(07) ADM=Locked
OML link established using TRX 0
setting Unit ID to '1801/0/0'
setting primary OML link IP to '10.9.1.154'
abis_nm.c:316 OC=CHANNEL(03) INST=(00,00,00) STATE CHG:
OP_STATE=Disabled AVAIL=Not installed(07) ADM=Locked
...
abis_nm.c:2433 OC=BASEBAND-TRANSCEIVER(04) INST=(00,00,ff) IPACCESS(0xf0):
SET NVATTR ACK
Set the NV Attributes.
```

❶ Unit ID

❷ IP address of the NITB

❸ IP address of the nanoBTS

2 Reviewing and Provisioning BTS configuration

The main functionality of the BSC component is to manage BTSs. As such, provisioning BTSs within the BSC is one of the most common tasks during BSC operation. Just like about anything else in OsmoBSC, they are configured using the VTY.

BTSs are internally numbered with integer numbers starting from "0" for the first BTS. BTS numbers have to be contiguous, so you cannot configure 0,1,2 and then 5.

2.1 Reviewing current BTS status and configuration

In order to view the status and properties of a BTS, you can issue the `show bts` command. If used without any BTS number, it will display information about all provisioned BTS numbers.


```
OpenBSC> show bts 0
BTS 0 is of nanobts type in band DCS1800, has CI 0 LAC 1, BSIC 63, TSC 7 and 1 TRX
Description: (null)
MS Max power: 15 dBm
Minimum Rx Level for Access: -110 dBm
Cell Reselection Hysteresis: 4 dBm
RACH TX-Integer: 9
RACH Max transmissions: 7
System Information present: 0x0000007e, static: 0x00000000
  Unit ID: 200/0/0, OML Stream ID 0xff
  NM State: Oper 'Enabled', Admin 2, Avail 'OK'
  Site Mgr NM State: Oper 'Enabled', Admin 0, Avail 'OK'
  Paging: 0 pending requests, 0 free slots
  OML Link state: connected.
  Current Channel Load:
                   TCH/F:   0% (0/5)
                  SDCCH8:   0% (0/8)
```

You can also review the status of the TRXs configured within the BTSs of this BSC by using `show trx`:

```
OpenBSC> show trx 0 0
TRX 0 of BTS 0 is on ARFCN 871
Description: (null)
  RF Nominal Power: 23 dBm, reduced by 0 dB, resulting BS power: 23 dBm
  NM State: Oper 'Enabled', Admin 2, Avail 'OK'
  Baseband Transceiver NM State: Oper 'Enabled', Admin 2, Avail 'OK'
  ip.access stream ID: 0x00
```

The output can be restricted to the TRXs of one specified BTS number (`show trx 0`) or even that of a single specified TRX within a specified BTS (`show trx 0 0`).

Furthermore, information on the individual timeslots can be shown by means of `show timeslot`. The output can be restricted to the timeslots of a single BTS (`show timeslot 0`) or that of a single TRX (`show timeslot 0 0`). Finally, you can restrict the output to a single timeslot by specifying the BTS, TRX and TS numbers (`show timeslot 0 0 4`).

```
OpenBSC> show timeslot 0 0 0
BTS 0, TRX 0, Timeslot 0, phys cfg CCCH, TSC 7
  NM State: Oper 'Enabled', Admin 2, Avail 'OK'
OpenBSC> show timeslot 0 0 1
BTS 0, TRX 0, Timeslot 1, phys cfg SDCCH8, TSC 7
  NM State: Oper 'Enabled', Admin 2, Avail 'OK'
```

2.2 Provisioning a new BTS

In order to provision BTSs, you have to enter the BTS config node of the VTY. In order to configure BTS 0, you can issue the following sequence of commands:

```
OpenBSC> enable
OpenBSC# configure terminal
OpenBSC(config)# network
OpenBSC(config-net)# bts 0
OpenBSC(config-net-bts)#
```

At this point, you have a plethora of commands, in fact an entire hierarchy of commands to configure all aspects of the BTS, as well as each of its TRX and each timeslot within each TRX. For a full reference, please consult the telnet VTY integrated help or the respective chapter in the VTY reference.

BTS configuration depends quite a bit on the specific BTS vendor and model. The section below provides just one possible example for the case of a sysmoBTS.

Note that from the `configure terminal` command onwards, the telnet VTY commands above are identical to configuration file settings, for details see Section 16.

Starting with `network` as above, your complete sysmoBTS configuration may look like this:

```
network
 bts 0
  type sysmobts
  band DCS1800
  description The new BTS in Baikonur
  location_area_code 2342
  cell_identity 5
  base_station_id_code 63
  ip.access unit_id 8888 0
  ms max power 40
  trx 0
   arfcn 871
   nominal power 23
   max_power_red 0
   timeslot 0
    phys_chan_config CCCH+SDCCH4
   timeslot 1
    phys_chan_config TCH/F
   timeslot 2
    phys_chan_config TCH/F
   timeslot 3
    phys_chan_config TCH/F
   timeslot 4
    phys_chan_config TCH/F
   timeslot 5
    phys_chan_config TCH/F
   timeslot 6
    phys_chan_config TCH/F
   timeslot 7
    phys_chan_config PDCH
```

2.3 System Information configuration

A GSM BTS periodically transmits a series of *SYSTEM INFORMATION* messages to mobile stations, both via the BCCH in idle mode, was well as via the SACCH in dedicated mode. There are many different types of such messages. For their detailed contents and encoding, please see *3GPP TS 24.008* [3gpp-ts-24-008].

For each of the *SYSTEM INFORMATION* message types, you can configure to have the BSC generate it automatically (*computed*), or you can specify the respective binary message as a string of hexadecimal digits.

The default configuration is to compute all (required) *SYSTEM INFORMATION* messages automatically.

Please see the *OsmoBSC VTY Reference Manual* [vty-ref-osmobsc] for further information, particularly on the following commands:

- `system-information (1|2|3|4|5|6|7|8|9|10|13|16|17|18|19|20|2bis|2ter|2quater|5bis|5ter) mode (static|computed)`
- `system-information (1|2|3|4|5|6|7|8|9|10|13|16|17|18|19|20|2bis|2ter|2quater|5bis|5ter) static HEXSTRING`

2.4 Neighbor List configuration

Every BTS sends a list of ARFCNs of neighbor cells . within its *SYSTEM INFORMATION 2* (and 2bis/2ter) messages on the BCCH . within its *SYSTEM INFORMATION 5* messages on SACCH in dedicated mode

For every BTS config node in the VTY, you can specify the behavior of the neighbor list using the `neighbor list mode` VTY command:

automatic
Automatically generate a list of neighbor cells using all other BTSs configured in the VTY

manual
Manually specify the neighbor list by means of `neighbor-list (add|del) arfcn <0-1023>` commands, having identical neighbor lists on BCCH (SI2) and SACCH (SI5)

manual-si5
Manually specify the neighbor list by means of `neighbor-list (add|del) arfcn <0-1023>` for BCCH (SI2) and a separate neighbor list by means of `si5 neighbor-list (add|del) arfcn <0-1023>` for SACCH (SI5).

2.5 Configuring GPRS PCU parameters of a BTS

In the case of BTS models using Abis/IP (IPA), the GPRS PCU is located inside the BTS. The BTS then establishes a Gb connection to the SGSN.

All the BTS-internal PCU configuration is performed via A-bis OML by means of configuring the *CELL*, *NSVC* (NS Virtual Connection and *NSE* (NS Entity).

There is one *CELL* node and one *NSE* node, but there are two *NSVC* nodes. At the time of this writing, only the NSVC 0 is supported by OsmoBTS, while both NSVC are supported by the ip.access nanoBTS.

The respective VTY configuration parameters are described below. They all exist beneath each BTS VTY config node.

But let's first start with a small example

Example configuration of GPRS PCU parameters at VTY BTS node

```
OpenBSC(config-net-bts)# gprs mode gprs
OpenBSC(config-net-bts)# gprs routing area 1
OpenBSC(config-net-bts)# gprs cell bvci 1234
OpenBSC(config-net-bts)# gprs nsei 1234
OpenBSC(config-net-bts)# gprs nsvc 0 nsvci 1234
OpenBSC(config-net-bts)# gprs nsvc 0 local udp port 23000
OpenBSC(config-net-bts)# gprs nsvc 0 remote udp port 23000
OpenBSC(config-net-bts)# gprs nsvc 0 remote ip 192.168.100.239
```

2.6 More explanation about the PCU config parameters

2.6.1 `gprs mode (none|gprs|egprs)`

This command determines if GPRS (or EGPRS) services are to be enabled in this cell at all.

2.6.2 `gprs cell bvci <2-65535>`

Configures the *BSSGP Virtual Circuit Identifier*. It must be unique between all BGSGP connections to one SGSN.

Note
It is up to the system administrator to ensure all PCUs are allocated an unique bvci. OsmoBSC will not ensure this policy.

2.6.3 gprs nsei <0-65535>

Configures the *NS Entity Identifier*. It must be unique between all NS connections to one SGSN.

Note
It is up to the system administrator to ensure all PCUs are allocated an unique bvci. OsmoBSC will not ensure this policy.

2.6.4 gprs nsvc <0-1> nsvci <0-65535>

Configures the *NS Virtual Connection Identifier*. It must be unique between all NS virtual connections to one SGSN.

Note
It is up to the system administrator to ensure all PCUs are allocated an unique nsvci. OsmoBSC will not ensure this policy.

2.6.5 gprs nsvc <0-1> local udp port <0-65535>

Configures the local (PCU side) UDP port for the NS-over-UDP link.

2.6.6 gprs nsvc <0-1> remote udp port <0-65535>

Configures the remote (SGSN side) UDP port for the NS-over-UDP link.

2.6.7 gprs nsvc <0-1> remote ip A.B.C.D

Configures the remote (SGSN side) UDP port for the NS-over-UDP link.

2.6.8 gprs ns timer (tns-block|tns-block-retries|tns-reset|tns-reset-retries|tns-test|tns-alive|tns-alive-retries) <0-255>

Configures the various GPRS NS related timers. Please check the GPRS NS specification for the detailed meaning of those timers.

2.7 Dynamic Timeslot Configuration (TCH / PDCH)

A dynamic timeslot is in principle a voice timeslot (TCH) that is used to serve GPRS data (PDCH) when no voice call is active on it. This enhances GPRS bandwidth while no voice calls are active, which is dynamically scaled down as voice calls need to be served. This is a tremendous improvement in service over statically assigning a fixed number of timeslots for voice and data.

The causality is as follows: to establish a voice call, the MSC requests a logical channel of a given TCH kind from the BSC. The BSC assigns such a channel from a BTS' TRX's timeslot of its choice. The knowledge that a given timeslot is dynamic exists only on the BSC level. When the MSC asks for a logical channel, the BSC may switch off PDCH on a dynamic timeslot and then assign a logical TCH channel on it. Hence, though compatibility with the BTS needs to be ensured, any MSC is compatible with dynamic timeslots by definition.

OsmoBSC and OsmoNITB support two kinds of dynamic timeslot handling, configured via the `network` / `bts` / `trx` / `time slot` / `phys_chan_config` configuration. Not all BTS models support dynamic channels.

Table 1: Dynamic timeslot support by various BTS models

Table 1: (continued)

	TCH/F_TCH/H_PDCH	TCH/F_PDCH
ip.access nanoBTS	-	supported
Ericsson RBS	supported	-
sysmoBTS using *osmo-bts-sysmo*	supported	supported
various SDR platforms using *osmo-bts-trx*	supported	supported
Nutaq Litecell 1.5 using *osmo-bts-litecell15*	supported	supported
Octasic OctBTS using *osmo-bts-octphy*	supported	supported

The *OsmoBTS Abis Protocol Specification* [osmobts-abis-spec] describes the non-standard RSL messages used for these timeslot kinds.

Note
Same as for dedicated PDCH timeslots, you need to enable GPRS and operate a PCU, SGSN and GGSN to provide the actual data service.

2.7.1 Osmocom Style Dynamic Timeslots (TCH/F_TCH/H_PDCH)

Timeslots of the TCH/F_TCH/H_PDCH type dynamically switch between TCH/F, TCH/H and PDCH, depending on the channel kind requested by the MSC. The RSL messaging for TCH/F_TCH/H_PDCH timeslots is compatible with Ericsson RBS.

BTS models supporting this timeslot kind are shown in Table 1.

In the lack of transcoding capabilities, this timeslot type may cause mismatching codecs to be selected for two parties of the same call, which would cause call routing to fail ("Cannot patch through call with different channel types: local = TCH_F, remote = TCH_H"). A workaround is to disable TCH/F on this timeslot type, i.e. to allow only TCH/H. To disable TCH/F on Osmocom style dynamic timeslots, use a configuration of

```
network
 dyn_ts_allow_tch_f 0
```

In OsmoNITB, disabling TCH/F on Osmocom dynamic timeslots is the default. In OsmoBSC, the default is to allow both.

2.7.2 ip.access Style Dynamic Timeslots (TCH/F_PDCH)

Timeslots of the TCH/F_PDCH type dynamically switch between TCH/F and PDCH. The RSL messaging for TCH/F_PDCH timeslots is compatible with ip.access nanoBTS.

BTS models supporting this timeslot kind are shown in Table 1.

2.7.3 Avoid PDCH Exhaustion

To avoid disrupting GPRS, configure at least one timeslot as dedicated PDCH. With only dynamic timeslots, a given number of voice calls would convert all timeslots to TCH, and no PDCH timeslots would be left for GPRS service.

2.7.4 Dynamic Timeslot Configuration Examples

This is an extract of an osmo-bsc or osmo-nitb config file. A timeslot configuration with five Osmocom style dynamic timeslots and one dedicated PDCH may look like this:


```
network
 bts 0
  trx 0
   timeslot 0
    phys_chan_config CCCH+SDCCH4
   timeslot 1
    phys_chan_config SDCCH8
   timeslot 2
    phys_chan_config TCH/F_TCH/H_PDCH
   timeslot 3
    phys_chan_config TCH/F_TCH/H_PDCH
   timeslot 4
    phys_chan_config TCH/F_TCH/H_PDCH
   timeslot 5
    phys_chan_config TCH/F_TCH/H_PDCH
   timeslot 6
    phys_chan_config TCH/F_TCH/H_PDCH
   timeslot 7
    phys_chan_config PDCH
```

With the ip.access nanoBTS, only `TCH/F_PDCH` dynamic timeslots are supported, and hence a nanoBTS configuration may look like this:

```
network
 bts 0
  trx 0
   timeslot 0
    phys_chan_config CCCH+SDCCH4
   timeslot 1
    phys_chan_config SDCCH8
   timeslot 2
    phys_chan_config TCH/F_PDCH
   timeslot 3
    phys_chan_config TCH/F_PDCH
   timeslot 4
    phys_chan_config TCH/F_PDCH
   timeslot 5
    phys_chan_config TCH/F_PDCH
   timeslot 6
    phys_chan_config TCH/F_PDCH
   timeslot 7
    phys_chan_config PDCH
```

3 Cell Broadcast

Normally, all user plane data in GSM/GPRS networks are sent in point-to-point channels from the network to the user. Those are called "dedicated" radio channels which exist between the network and one given phone/subscriber at a time.

Cell Broadcast is an exception to that rule. It permits user data (so-called SMS-CB data) to be broadcast by the network in a way that can be received by all phones in the coverage area of the given BTS simultaneously.

More high-level information can be found at https://en.wikipedia.org/wiki/Cell_Broadcast and the related specification is [?].

3.1 Use Cases

Cell Broadcast was used for various different use cases primarily in the 1990ies and early 2000s, including

- advertisement of the GPS position of the cell tower you're currently camping on

- advertisement of the calling codes of your current "home zone", i.e. a "lower cost short distance" call zone travelling with you as you roam around.

More recently, SMS-CB is seeing some uptake by various disaster warning systems, such as

- CMAS (Commercial Mobile Alert System), later renamed to WEA (Wireless Emergency Alerts) in the US.
- EU-Alert in the European union
- Messer Ishi (Rocket Alert) in Israel
- ETWS (Earthquake and Tsunami Warning System) in Japan
- KPAS (Korean Public Alert System)

3.2 Osmocom Cell Broadcast support

- OsmoBTS implements the "SMS BROADCAST COMMAND" Message in RSL according to Section 8.5.8 of 3GPP TS 08.58
- OsmoNITB and OsmoBSC implement a VTY command `bts <0-255> smscb-command <1-4> HEXSTRING` to send a given hex-formatted cell broadcast message to a specified BTS

3.2.1 What's missing

What's missing (for production operation in larger networks)

- mechanism to broadcast one (set of) cell broadcast messages from the BSC to multiple/all BTSs, rather than one BTS individually
- OsmoBTS reporting of current CBCH load
- BSC scheduler scheduling multiple alternating sets of CBCH messages based on the current CBCH load reported by BTS
- external interface from BSC to a Cell Broadcast Center (CBC), e.g. according to 3GPP TS 48.049
- an Osmocom implementation of the Cell Broadcast Center (OsmoCBC) which can manage and distribute messages to multiple BSCs and which has an external interface by which cell-broadcast can be entered into the network

If you would like to contribute in any of those areas (by means of code or funding), please reach out to us any time.

3.3 Message Structure

- Each message has a meximum of 15 pages
- Each page is 82 bytes of data, resulting in 93 characters in GSM 7-bit default alphabet
- Messages are broadcast on logical channels (more like an address)
- Subscribers can activate/deactivate selective addresses

4 Osmocom Control Interface

The VTY interface as described in Section 16 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.

4.1 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).

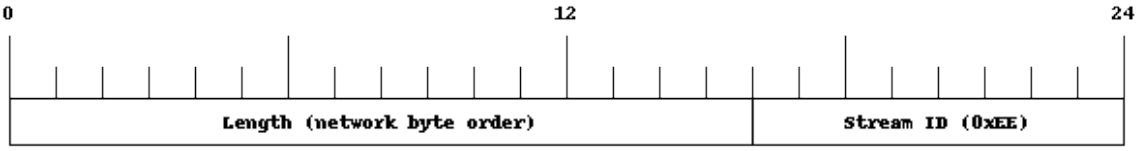


Figure 1: IPA header for control protocol

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

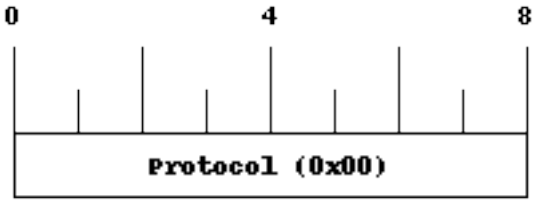


Figure 2: IPA extension header for control protocol

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.

4.1.1 GET operation

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

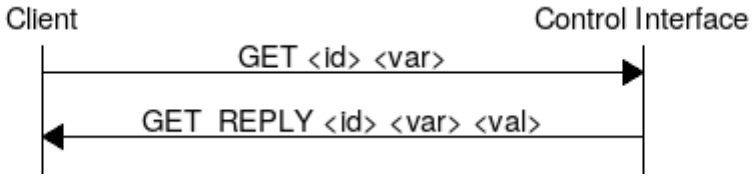


Figure 3: Control Interface GET operation (successful outcome)

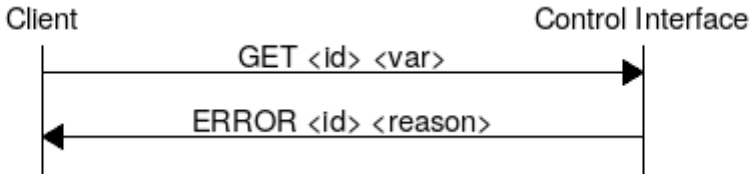


Figure 4: Control Interface GET operation (unsuccessful outcome)

4.1.2 SET operation

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

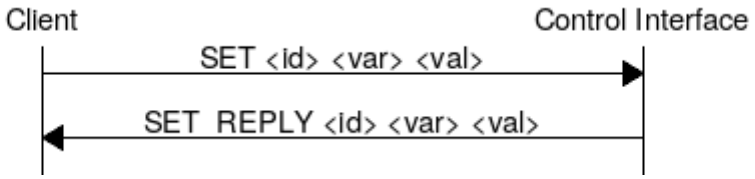


Figure 5: Control Interface SET operation (successful outcome)

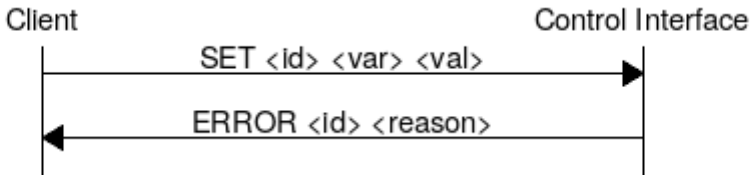


Figure 6: Control Interface SET operation (unsuccessful outcome)

4.1.3 TRAP operation

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

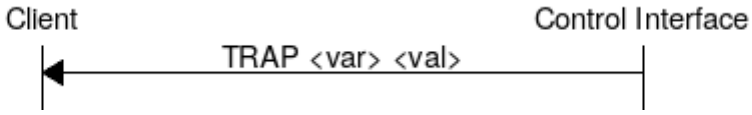


Figure 7: Control Interface TRAP operation

4.2 Common variables

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

Table 2: Variables available over control interface

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

Those read-only variables allow to get value of arbitrary counter using its name.

For example "`rate_ctr.per_hour.bsc.0.handover:timeout`" is the number of handover timeouts per hour.

Of course for that to work the program in question have to register corresponding counter names and groups using libosmocore functions.

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

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

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

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

4.3 Control Interface python examples

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

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

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

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

4.3.1 Getting rate counters

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

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

4.3.2 Setting a value

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

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

4.3.3 Getting a value

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

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

4.3.4 Listening for traps

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

Example: Using osmo_ctrl.py to listen for traps:

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

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

4.4 Gb interface configuration

4.4.1 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

4.4.2 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

4.4.3 NS Timer configuration

The NS protocol features a number of configurable timers.

Table 3: 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

4.5 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

4.6 FIXME

4.6.1 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.

4.7 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
```


5 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

GT
Global Title; an address in SCCP

GTP
GPRS Tunnel Protocol; used between SGSN and GGSN

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

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

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

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

M3UA
MTP3 User Adaptation; a SIGTRAN Variant (*RFC 4666* [ietf-rfc4666])

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

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

MGW
Media Gateway

MM
Mobility Management; part of the GSM Layer 3 Protocol

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

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

MTP
Message Transfer Part; SS7 signaling protocol (*ITU-T Q.701* [itu-t-q701])

MVNO
Mobile Virtual Network Operator; Operator without physical radio network

NCC
Network Color Code; assigned by national regulator

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

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

PC
Point Code; an address in MTP

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

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

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

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

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

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

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

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

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

RF
Radio Frequency

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

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

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

RR
Radio Resources; Part of the GSM Layer 3 Protocol

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

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

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

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

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

SDK
Software Development Kit

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

SIM
Subscriber Identity Module; small chip card storing subscriber identity

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

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

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

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

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

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

STP
Signaling Transfer Point; A Router in SS7 Networks

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

syslog
System logging service of UNIX-like operating systems

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

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

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

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

TRX
Transceiver; element of a BTS serving a single carrier

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

6 Generic Subscriber Update Protocol

6.1 General

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

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

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

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

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

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

6.2 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.

6.3 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*.

6.4 Procedures

6.4.1 Authentication management

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

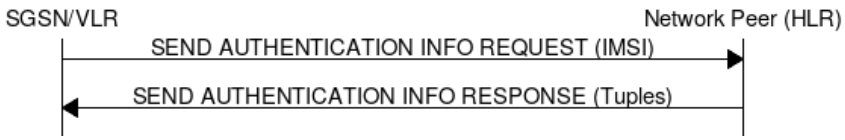


Figure 8: Send Authentication Info (Normal Case)

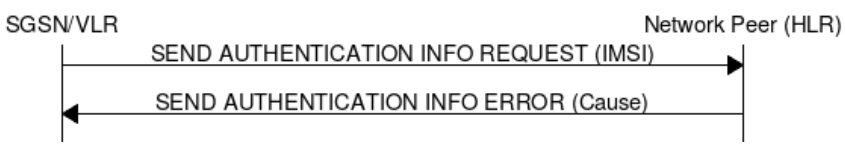


Figure 9: Send Authentication Info (Erroneous Case)

6.4.2 Reporting of Authentication Failure

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

Figure 10: Authentication Failure Report (Normal Case)

6.4.3 Location Updating

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

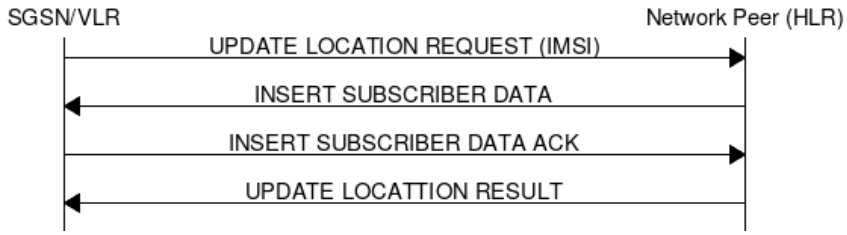


Figure 11: Update Location (Normal Case)

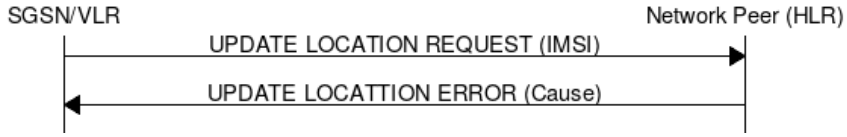


Figure 12: Update Location (Error Case)

6.4.4 Location Cancellation

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

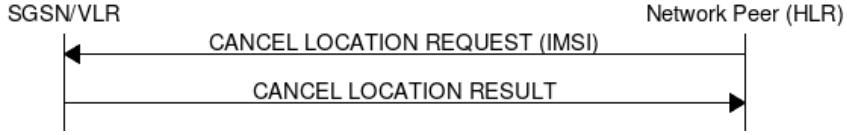


Figure 13: Cancel Location (Normal Case)

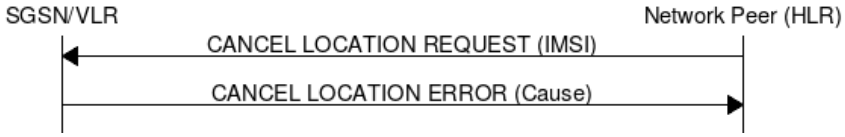


Figure 14: Cancel Location (Error Case)

6.4.5 Purge MS

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

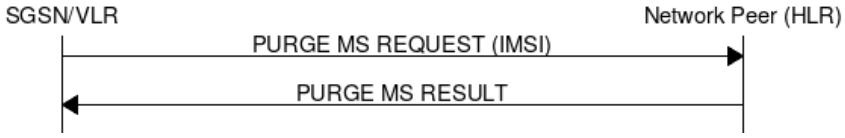


Figure 15: Purge MS (Normal Case)

6.4.6 Delete Subscriber Data

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

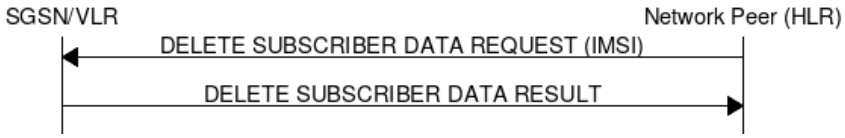


Figure 16: Delete Subscriber Data (Normal Case)

6.5 Message Format

6.5.1 General

Every message is based on the following message format

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	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.

6.5.2 Send Authentication Info Request

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3
26	AUTS	Section 6.6.13	C	TLV	18
20	RAND	Section 6.6.7	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.

6.5.3 Send Authentication Info Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
02	Cause	Section 6.6.25	M	TLV	3

6.5.4 Send Authentication Info Response

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
03	Auth Tuple	Section 6.6.6	0-5	TLV	36

6.5.5 Authentication Failure Report

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3

6.5.6 Update Location Request

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3

6.5.7 Update Location Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10

IEI	IE	Type	Presence	Format	Length
02	Cause	Section 6.6.25	M	TLV	3

6.5.8 Update Location Result

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
08	MSISDN	Section 6.6.20	O	TLV	0-9
09	HLR Number	Section 6.6.24	O	TLV	0-9
04	PDP info complete	Section 6.6.18	O	TLV	2
05	PDP info	Section 6.6.3	1-10	TLV	

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

6.5.9 Location Cancellation Request

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3
06	Cancellation type	Section 6.6.16	O	TLV	3

6.5.10 Location Cancellation Result

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3

6.5.11 Purge MS Request

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3
09	HLR Number	Section 6.6.24	M	TLV	0-9

6.5.12 Purge MS Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10

IEI	IE	Type	Presence	Format	Length
02	Cause	Section 6.6.25	M	TLV	3

6.5.13 Purge MS Result

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
07	Freeze P-TMSI	Section 6.6.18	M	TLV	2

6.5.14 Insert Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
28	CN Domain	Section 6.6.15	O	TLV	3
08	MSISDN	Section 6.6.20	O	TLV	0-9
09	HLR Number	Section 6.6.24	O	TLV	0-9
04	PDP info complete	Section 6.6.18	M	TLV	2
05	PDP info	Section 6.6.3	0-10	TLV	
14	PDP-Charging Characteristics	Section 6.6.23	O	TLV	4

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

6.5.15 Insert Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
02	Cause	Section 6.6.25	M	TLV	3

6.5.16 Insert Subscriber Data Result

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10

6.5.17 Delete Subscriber Data Request

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10

IEI	IE	Type	Presence	Format	Length
28	CN Domain	Section 6.6.15	O	TLV	3
10	PDP context id	Section 6.6.3 (no conditional IE)	0-10	TLV	

6.5.18 Delete Subscriber Data Error

Direction: SGSN / VLR ⇒ HLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
02	Cause	Section 6.6.25	M	TLV	3

6.5.19 Delete Subscriber Data Result

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10

6.5.20 Process Supplementary Service Request

Direction: bidirectional

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
30	Session ID	Section 6.7.1	M	TLV	6
31	Session State	Section 6.7.2	M	TLV	3
35	Supplementary Service Info	Section 6.6.26	O	TLV	2-...

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

6.5.21 Process Supplementary Service Error

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1
01	IMSI	Section 6.6.19	M	TLV	2-10
30	Session ID	Section 6.7.1	M	TLV	6
31	Session State	Section 6.7.2	M	TLV	3
02	Cause	Section 6.6.25	M	TLV	3

6.5.22 Process Supplementary Service Response

Direction: HLR ⇒ SGSN / VLR

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 6.6.1	M	V	1

IEI	IE	Type	Presence	Format	Length
01	IMSI	Section 6.6.19	M	TLV	2-10
30	Session ID	Section 6.7.1	M	TLV	6
31	Session State	Section 6.7.2	M	TLV	3
35	Supplementary Service Info	Section 6.6.26	O	TLV	2-...

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

6.6 Information Elements

6.6.1 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
0x1c	Location Cancellation Request
0x1d	Location Cancellation Error
0x1e	Location Cancellation Result
0x20	Supplementary Service Request
0x21	Supplementary Service Error
0x22	Supplementary Service Result

6.6.2 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*.

6.6.3 PDP Info

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

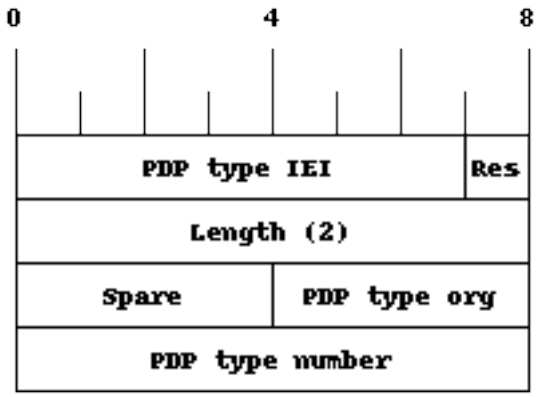
IEI	IE	Type	Presence	Format	Length
	PDP Info IEI	Section 6.6.17	M	V	1
	Length of PDP Info IE		M	V	1
10	PDP Context ID	Section 6.6.5	C	TLV	3
11	PDP Type	Section 6.6.4	C	TLV	4

IEI	IE	Type	Presence	Format	Length
12	Access Point Name	Section 6.6.21	C	TLV	3-102
13	Quality of Service	Section 6.6.22	O	TLV	1-20
14	PDP-Charging Characteristics	Section 6.6.23	O	TLV	4

The conditional IE are mandantory unless mentioned otherwise.

6.6.4 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.



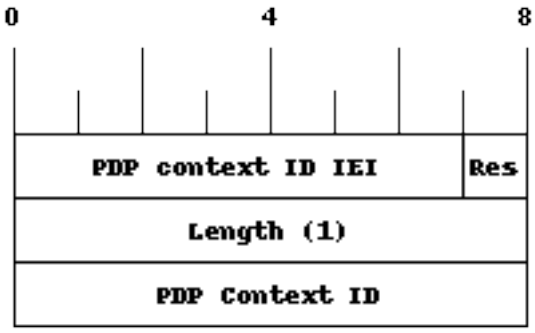
The spare bits are left undefined. While 09.60 defines them as *1 1 1 1*, there are MAP traces where these bits are set to *0 0 0 0*. So the receiver shall ignore these bits.

Examples:

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

6.6.5 PDP Context ID

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



6.6.6 Auth tuple

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

IEI	IE	Type	Presence	Format	Length
	Auth Tuple IEI	Section 6.6.17	M	V	1
	Length of Auth Tuple IE		M	V	1
20	RAND	Section 6.6.7	M	TLV	18
21	SRES	Section 6.6.8	M	TLV	6
22	Kc	Section 6.6.9	M	TLV	10
23	IK	Section 6.6.10	C	TLV	18
24	CK	Section 6.6.11	C	TLV	18
25	AUTN	Section 6.6.12	C	TLV	18
27	RES	Section 6.6.14	C	TLV	2-18

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

6.6.7 RAND

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

6.6.8 SRES

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

6.6.9 Kc

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

6.6.10 IK

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

6.6.11 CK

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

6.6.12 AUTN

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

6.6.13 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.

6.6.14 RES

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

6.6.15 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 4: CN Domain Number

Type	Description
0x01	PS Domain
0x02	CS Domain

6.6.16 Cancellation Type

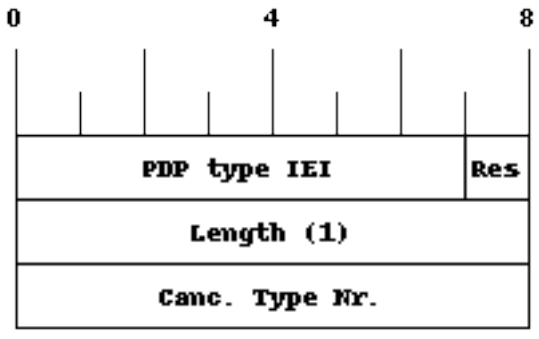


Table 5: Cancellation Type Number

Number	Description
0x00	Update Procedure
0x01	Subscription Withdrawn

6.6.17 IE Identifier (informational)

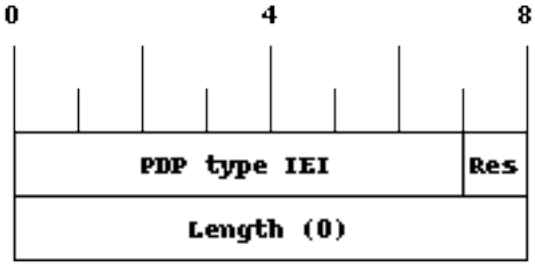
These are the standard values for the IEI. See the message definitions for the IEI that shall be used for the encoding.

Table 6: GSUP IE Identifiers

IEI	Info Element	Type / Encoding
0x01	IMSI	Mobile Identity, 3GPP TS 04.08 Ch. 10.5.1.4
0x02	Cause	Section 6.6.25
0x03	Auth Tuple	Section 6.6.6
0x04	PDP Info Compl	Section 6.6.18
0x05	PDP Info	Section 6.6.3
0x06	Cancel Type	Section 6.6.16
0x07	Freeze P-TMSI	Section 6.6.18
0x08	MSISDN	ISDN-AddressString/octet, Section 6.6.20
0x09	HLR Number	Section 6.6.24
0x10	PDP Context ID	Section 6.6.5
0x11	PDP Type	Section 6.6.4
0x12	Access Point Name	Section 6.6.21
0x13	QoS	Section 6.6.22
0x14	PDP-Charging Characteristics	Section 6.6.23
0x20	RAND	Section 6.6.7
0x21	SRES	Section 6.6.8
0x22	Kc	Section 6.6.9
0x23	IK	Section 6.6.10
0x24	CK	Section 6.6.11
0x25	AUTN	Section 6.6.12
0x26	AUTS	Section 6.6.13
0x27	RES	Section 6.6.14
0x28	CN Domain	Section 6.6.15
0x30	Session ID	Section 6.7.1
0x31	Session State	Section 6.7.2
0x35	Supplementary Service Info	Section 6.6.26

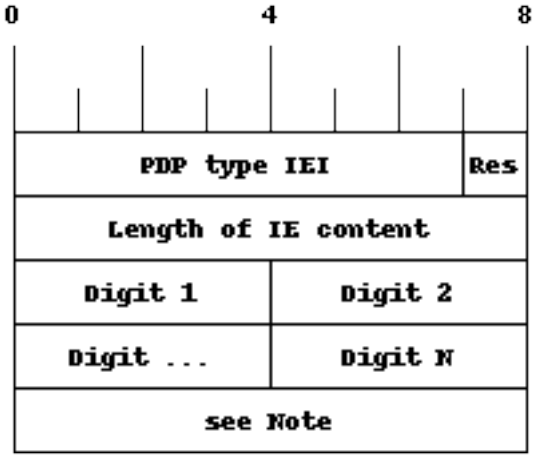
6.6.18 Empty field

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.



6.6.19 IMSI

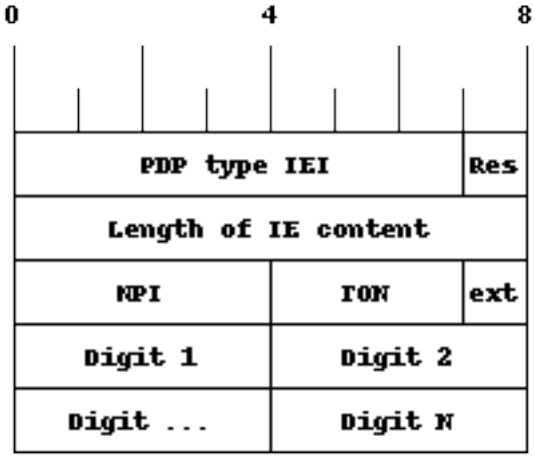
The IMSI is encoded like in octet 4-N of the Called Party BCD Number defined in 3GPP TS 04.08, 10.5.4.7.



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.

6.6.20 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 or VLR and then passed as is to the GGSN during the activation of the primary PDP Context.

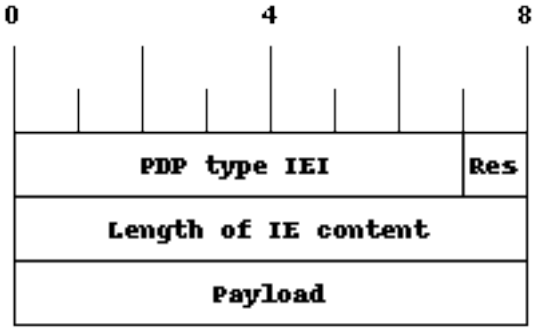


6.6.21 Access Point Name

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

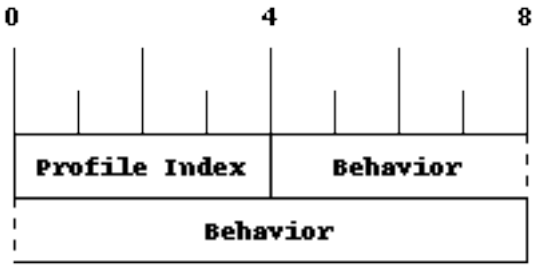
6.6.22 Quality of Service Subscribed Service

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.



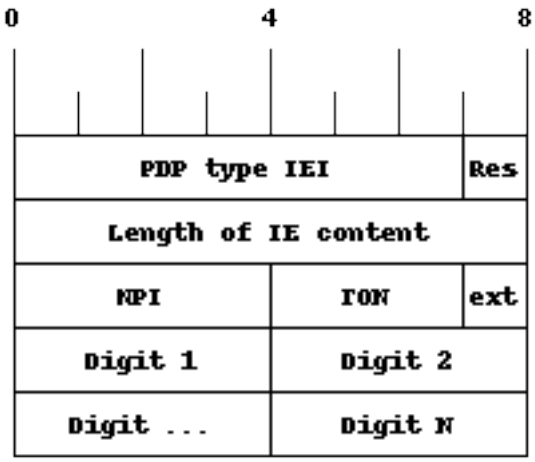
6.6.23 PDP-Charging Characteristics

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 or VLR when activating a PDP context.



6.6.24 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 or VLR can be used by the CDR module to keep a record.



6.6.25 Cause

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

6.6.26 Supplementary Service Info

This IE shall be used together with both Section 6.7.2 and Section 6.7.1 IEs. It is used to carry the payload of Supplementary Services encoded according to GSM TS 04.80.

6.7 Session (transaction) management

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

6.7.1 Session ID

This auxiliary IE shall be used together with Section 6.7.2. The purpose of this IE is to identify a particular transaction using the 4-byte unique identifier.

6.7.2 Session State

This auxiliary IE shall be used together with Section 6.7.1. The purpose of this IE is to indicate a state of a particular transacrion, i.e. initiate, continue or terminate it.

Table 7: Session state

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

7 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.

7.1 Log categories

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

7.2 Log levels

For each of the log categories (see Section 7.1), you can set an independent log level, controlling the level of verbosity. Log levels include:

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

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

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

info
Some information about normal/regular system activity is provided.

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

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

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

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

Afterwards you can adjust specific categories as usual.

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

7.3 Log printing options

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

log color 1
With this option each log message will log with the color of its category. The color is hard-coded and can not be changed. As with other options a *0* disables this functionality.

log timestamp 1
Includes the current time in the log message. When logging to syslog this option should not be needed, but may come in handy when debugging an issue while logging to file.

log print extended-timestamp 1
In order to debug time-critical issues this option will print a timestamp with millisecond granularity.

log print category 1
Prefix each log message with the category name.

log print category-hex 1
Prefix each log message with the category number in hex (<*000b*>).

log print level 1
Prefix each log message with the name of the log level.

log print file 1
Prefix each log message with the source file and line number. Append the keyword `last` to append the file information instead of prefixing it.

7.4 Log filters

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

To request no filtering, i.e. see all messages, you may use: `log filter all 1`

In addition to generic filtering, applications can implement special log filters using the same framework to filter on particular context.

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

7.5 Log targets

Each of the log targets represent certain destination for log messages. It can be configured independently by selecting levels (see Section 7.2) for categories (see Section 7.1) as well as filtering (see Section 7.4) and other options like `logging timestamp` for example.

7.5.1 Logging to the VTY

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

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

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

Next, you can configure the log levels for desired categories in your VTY session. See Section 7.1 for more details on categories and Section 7.2 for the log level details.

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

Finally, after having configured the levels, you still need to set the filter as it's described in Section 7.4.

Tip

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

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

7.5.2 Logging to the ring buffer

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

It's configured as follows:

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

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

7.5.3 Logging via gsmtap

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

It's configured as follows:

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

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

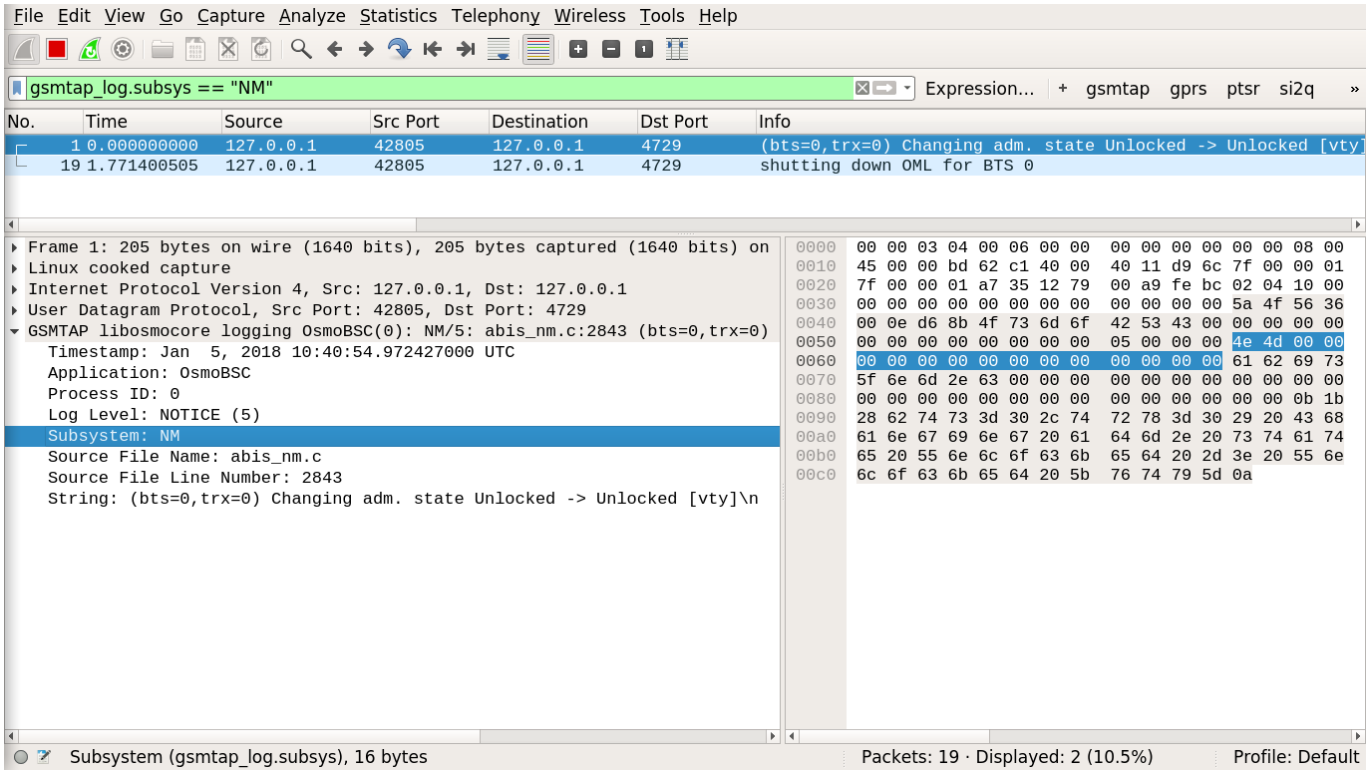


Figure 17: Wireshark with logs delivered over GSMTAP

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

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

7.5.4 Logging to a file

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

regarding levels / subsystems.

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

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

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

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

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

7.5.5 Logging to syslog

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

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

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

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

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

7.5.6 Logging to stderr

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

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

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


8 MNCC for External Call Control

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

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

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

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

Test can run in two different modes:

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

8.1 Internal MNCC handler

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

Note
Internal MNCC is the default behavior.

8.1.1 Internal MNCC Configuration

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

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

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

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

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

8.2 External MNCC handler

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

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

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

8.3 DTMF considerations

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

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

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

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

Note

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

8.4 MNCC protocol description

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

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

The different calls in the network are distinguished by their callref (call reference), which is a unique unsigned 32bit integer.

8.4.1 MNCC_HOLD_IND

Direction: Test → Handler

A *CC HOLD* message was received from the MS.

8.4.2 MNCC_HOLD_CNF

Direction: Handler → Test

Acknowledge a previously-received *CC HOLD* message, causes the transmission of a *CC HOLD ACK* message to the MS.

8.4.3 MNCC_HOLD_REJ

Direction: Handler → Test

Reject a previously-received *CC HOLD* message, causes the transmission of a *CC HOLD REJ* message to the MS.

8.4.4 MNCC_RETRIEVE_IND

Direction: Test → Handler

A *CC RETRIEVE* message was received from the MS.

8.4.5 MNCC_RETRIEVE_CNF

Direction: Handler → Test

Acknowledge a previously-received *CC RETRIEVE* message, causes the transmission of a *CC RETRIEVE ACK* message to the MS.

8.4.6 MNCC_RETRIEVE_REJ

Direction: Handler → Test

Reject a previously-received *CC RETRIEVE* message, causes the transmission of a *CC RETRIEVE REJ* message to the MS.

8.4.7 MNCC_USERINFO_REQ

Direction: Test → Handler

Causes a *CC USER INFO* message to be sent to the MS.

8.4.8 MNCC_USERINFO_IND

Direction: Test → Handler

Indicates that a *CC USER-USER* message has been received from the MS.

8.4.9 MNCC_BRIDGE

Direction: Handler → Test

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

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

8.4.10 MNCC_FRAME_RECV

Direction: Handler → Test

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

8.4.11 MNCC_FRAME_DROP

Direction: Handler → Test

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

8.4.12 MNCC_LCHAN_MODIFY

Direction: Handler → Test

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

8.4.13 MNCC_RTP_CREATE

Direction: Handler → Test

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

8.4.14 MNCC_RTP_CONNECT

Direction: Handler → Test

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

8.4.15 MNCC_RTP_FREE

Direction: Handler → Test

Release a RTP connection for one given call.

8.4.16 GSM_TCHF_FRAME

Direction: both

Transfer the payload of a GSM Full-Rate (FR) voice frame between the Test and an external MNCC handler.

8.4.17 GSM_TCHF_FRAME_EFR

Direction: both

Transfer the payload of a GSM Enhanced Full-Rate (EFR) voice frame between the Test and an external MNCC handler.

8.4.18 GSM_TCHH_FRAME

Direction: both

Transfer the payload of a GSM Half-Rate (HR) voice frame between the Test and an external MNCC handler.

8.4.19 GSM_TCH_FRAE_AMR

Direction: both

Transfer the payload of a GSM Adaptive-Multi-Rate (AMR) voice frame between the Test and an external MNCC handler.

8.4.20 GSM_BAD_FRAME

Direction: Test → Handler

Indicate that no valid voice frame, but a *bad frame* was received over the radio link from the MS.

8.4.21 MNCC_START_DTMF_IND

Direction: Test → Handler

Indicate the beginning of a DTMF tone playback.

8.4.22 MNCC_START_DTMF_RSP

Direction: Handler → Test

Acknowledge that the DTMF tone playback has been started.

8.4.23 MNCC_START_DTMF_REJ

Direction: both

Indicate that starting a DTMF tone playback was not possible.

8.4.24 MNCC_STOP_DTMF_IND

Direction: Test → Handler

Indicate the ending of a DTMF tone playback.

8.4.25 MNCC_STOP_DTMF_RSP

Direction: Handler → Test

Acknowledge that the DTMF tone playback has been stopped. == Osmocom Authentication Protocol (OAP)

8.5 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.

8.6 Connection

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

8.7 Using IPA

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

8.8 Procedures

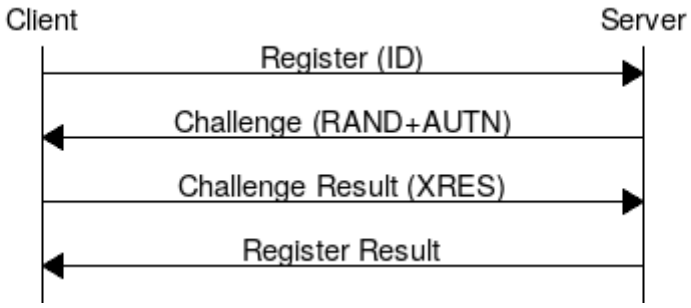


Figure 18: Ideal communication sequence

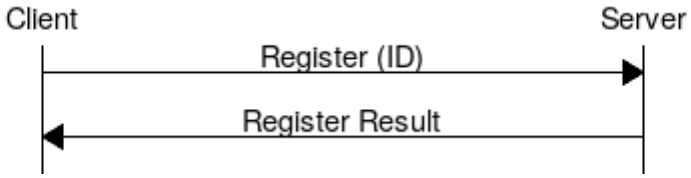


Figure 19: Variation "test setup"

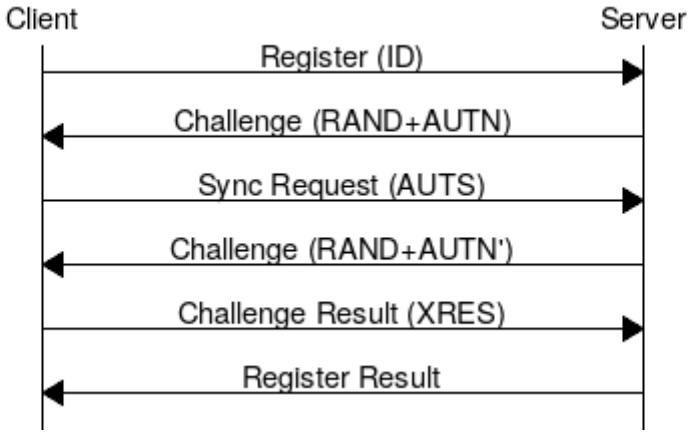


Figure 20: Variation "invalid sequence nr":

8.8.1 Register

The client sends a REGISTER_REQ message containing an identifier number.

8.8.2 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.

8.8.3 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.

8.8.4 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.

8.8.5 Sync Result

If the server has received a valid Sync Request, it shall answer by directly sending another Challenge (see Section 8.8.2). If an invalid Sync Request is received, the server shall reply with a REGISTER_ERR message.

8.8.6 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.

8.9 Message Format

Every message is based on the following message format

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1

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

8.9.1 Register Request

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1
30	Client ID	Section 8.10.3	M	TLV	4

8.9.2 Register Error

Direction: Server → Client

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1
02	Cause	GMM Cause, TS 04.08: 10.5.5.14	M	TLV	3

8.9.3 Register Result

Direction: Server → Client

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1

8.9.4 Challenge

Direction: Server → Client

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1
20	RAND	octet string (16)	TLV	18	23

8.9.5 Challenge Error

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1
02	Cause	GMM Cause, TS 04.08: 10.5.5.14	M	TLV	3

8.9.6 Challenge Result

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1

8.9.7 Sync Request

Direction: Client → Server

IEI	IE	Type	Presence	Format	Length
	Message Type	Section 8.10.1	M	V	1

8.9.8 Sync Error

Not used.

8.9.9 Sync Result

Not used.

8.10 Information Elements

8.10.1 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)

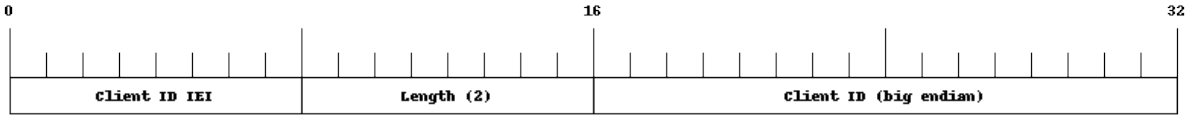
8.10.2 IE Identifier (informational)

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

IEI	Info Element	Type
0x24	XRES	Octet String
0x25	AUTS	Octet String
0x30	Client ID	big endian integer, 16 bit

8.10.3 Client ID



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

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

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

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

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

It has been a most exciting ride during the last eight-odd years. I would not have wanted to miss it under any circumstances.

— Harald Welte, Osmocom.org and OpenBSC founder, December 2017.

9.1 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.

9.2 Endorsements

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

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

10 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.

10.1 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.

10.2 Osmocom and sysmocom

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

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

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

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

10.3 Corrections

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

10.4 Legal disclaimers

10.4.1 Spectrum License

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

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

10.4.2 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.

10.4.3 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.*

10.4.4 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.

10.4.5 Documentation License

Please see Appendix B for further information.

11 Introduction

11.1 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 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

11.2 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. == Introduction into RF Electronics

Setup and Operation of a GSM network is not only about the configuration and system administration on the network elements and protocol stack, but also includes the physical radio transmission part.

Basic understanding about RF (Radio Frequency) Electronics is key to achieving good performance of the GSM network.

11.3 Coaxial Cabling

Coaxial cables come in many different shapes, diameters, physical construction, dielectric materials, and last but not least brands and types.

There are many parameters that might be relevant to your particular installation, starting from mechanical/environmental properties such as temperature range, UV resilience, water/weatherproofness, flammability, etc.

For the subject of this manual, we will not look at those mechanical properties, but look at the electrical properties instead.

The prime electrical parameters of a coaxial cable are:

- its attenuation over frequency and length
- its maximum current/power handling capability
- its propagation velocity (ignored here)
- its screening efficiency (ignored here)

11.3.1 Coaxial Cable Attenuation

The attenuation of a coaxial cable is given in dB per length, commonly in *dB per 100m*. This value changes significantly depending on the frequency of the signal transmitted via the cable. Cable manufacturers typically either provide tables with discrete frequency values, or graphs plotting the attenuation per 100m (x axis) over the frequency (y axis).

FIXME: Example.

So in order to estimate the loss of a coaxial cable, you need to

1. determine the frequency at which you will use the cable, as determined by the GSM frequency band of your BTS. Make sure you use the highest frequency that might occur, which is typically the upper end of the transmit band, see [?]
2. determine the attenuation of your cable per 100m at the given frequency (check the cable data sheet)

3. scale that value by the actual length of the cable

A real cable always has connectors attached to it, please add some additional losses for the connectors that are attached. 0.05 dB per connector is a general rule of thumb for the frequencies used in GSM.

FIXME: Example computation

As you can see very easily, the losses incurred in coaxial cables between your antenna and the BTS can very quickly become significant factors in your overall link budget (and thus cell coverage). This is particularly relevant for the uplink power budget. Every dB you loose in the antenna cable between antenna and the BTS receiver translates into reduced uplink coverage.

Using the shortest possible coaxial cabling (e.g. by mounting the BTS high up on the antenna tower) and using the highest-quality cabling are the best strategies to optimize

Warning
If you plan to assemble the coaxial connectors yourself, please make sure you ensure to have the right skills for this. Properly assembling coaxial connectors (whether solder-type or crimp-type) requires precision tools and strict process as described by the manufacturer. Any mechanical imprecision of connector assembly will cause significant extra signal attenuation.

11.3.2 Checking coaxial cables

If you would like to check the proper operation of a coaxial cable, there are several possible methods available:

- The more expensive method would be to use a *RF Network Analyzer* to measure the S11/S12 parameters or the VSWR of the cable.
- Another option is to use a TDR (time domain reflectometer) to determine the VSWR. The TDR method has the added advantage that you can localize any damage to the cable, as such damage would cause reflections that can be converted into meters cable length from the port at which you are testing the cable. Mobile, battery-powered TDR for field-use in GSM Site installation are available from various vendors. One commonly used series is the *Anritsu Site Master*.

11.4 Coaxial Connectors

A coaxial connector is a connector specifically designed for mounting to coaxial cable. It facilitates the removable / detachable connection of a coaxial cable to a RF device.

There are many different types of coaxial connectors on the market.

The most important types of coaxial connectors in the context of GSM BTSs are:

- The *N type* connector
- The *SMA type* connector.
- The *7/16* type connector

FIXME: Images

The above connectors are tightened by a screw-on shell. Each connector type has a specific designated nominal torque by which the connector shall be tightened. In case of uncertainty, please ask your connector supplier for the nominal torque.

Note
Always ensure the proper mechanical condition of your RF connectors. Don't use RF connectors that are contaminated by dust or dirt, or which show significant oxidization, bent contacts or the like. Using such connectors poses significant danger of unwanted signal loss, and can in some cases even lead to equipment damage (e.g. in case of RF power at PA output being reflected back into the PA).

11.5 Duplexers

A GSM BTS (or GSM TRX inside a BTS) typically exposes separate ports for Rx (Receive) and Tx (Transmit). This is intentionally the case, as this allows the users to add e.g. additional power amplifiers, filters or other external components into the signal path. Those components typically operate on either the receive or the transmit path.

You could now connect two separate antennas to the two ports (one for Rx, one for Tx). This is commonly done in indoor installations with small rubber-type antennas directly attached to the BTS connectors.

In outdoor installations, you typically (want to) use a single Antenna for Rx and Tx. This single antenna needs to be connected to the BTS via a device that is called *Duplexer*.

The *Duplexer* is actually a frequency splitter/combiner, which is specifically tuned to the uplink and downlink frequencies of the GSM band in which you operate the BTS. As such, it has one port that passes only uplink frequencies between the antenna and that port, as well as another port that passes only downlink frequencies between antenna and that port.

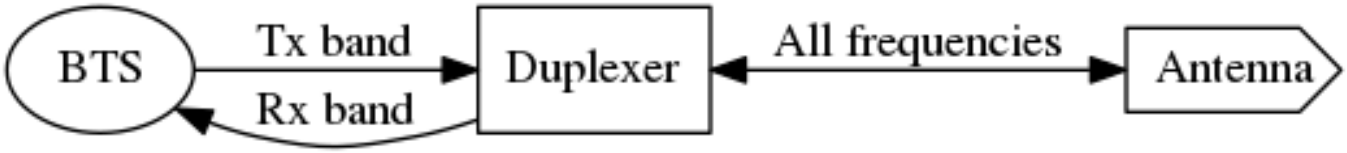


Figure 21: Illustration of the Duplexer functionality

Warning
The ports of a duplexer are not interchangeable. Always make sure that you use the Rx port of the duplexer with the Rx port of the BTS, and vice-versa for Tx.

11.6 RF Power Amplifiers

A RF Power Amplifier (PA) is a device that boosts the transmit power of your RF signal, the BTS in your case.

RF power amplifiers come in many different characteristics. Some of the key characteristics are:

Frequency range
A PA is typically designed for a specific frequency range. Only signals inside that range will be properly amplified

Gain in dB
This tells you how many dB the power amplifier will increase your signal. `Pout = Pin + Gain`

Maximum Output Power
This indicates the maximum absolute output power. For example, if the maximum output power is 40 dBm, and the gain is 10dBm, then an input signal of 30dBm will render the maximum output power. An input signal of 20dBm would subsequently generate only 30dBm of output power.

Efficiency
The efficiency determines how much electrical power is consumed for the given output power. Often expressed as Power Added Efficiency (PAE).

Warning
If you add external power amplifiers to a GSM BTS or any other transmitter, this will invalidate the regulatory approval of the BTS. It is your responsibility to ensure that the combination of BTS and PA still fulfills all regulatory requirements, for example in terms of out-of-band emissions, spectrum envelope, phase error, linearity, etc!

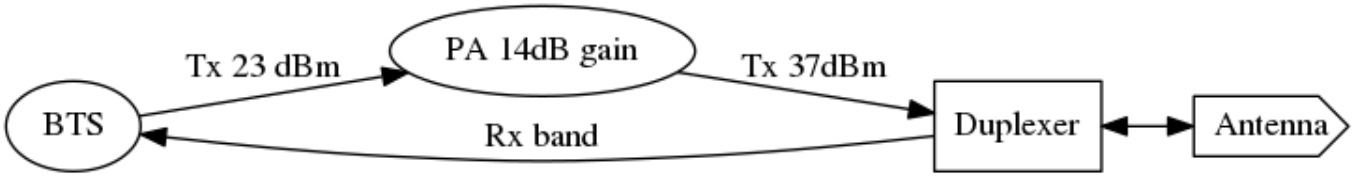


Figure 22: Addition of a RF Power Amplifier to a GSM BTS Setup

11.7 Antennas

The Antenna is responsible for converting the electromagnetic waves between the coaxial cable and the so-called *air interface* and vice-versa. The properties of an antenna are always symmetric for both transmission and reception.

Antennas come in many different types and shapes. Key characteristics distinguishing antennas are:

Antenna Gain
Expresses how much more efficient the antenna converts between cable and air interface. Can be expressed in dB compared to a theoretical isotropic radiator (dBi) or compared to a dipole antenna (dBd). Gain usually implies directivity.

Frequency Band(s)
Antennas typically have only a relatively narrow band (or multiple narrow bands at which they radiate efficiently. In general, the higher the antenna gain, the lower the usable frequency band of the antenna.

Directivity
Antennas radiate the energy in all three dimensions.

Mechanical Size
Mechanical Size is an important factor depending on how and where the antenna is mounted. Size also relates to weight and wind-load.

Wind Load
Expresses how much mechanical load the antenna will put on its support structure (antenna mast).

Connector Type
Your cabling will have to use a compatible connector for the antenna. Outdoor antennas typically use the 7/16 type connector or an N type connector. Indoor antennas either N type or SMA type.

Environmental Rating
Indoor antennas cannot be used outdoor, as they do not offer the level of protection against dust and particularly water / humidity / corrosion.

Down-tilt Capability
Particularly sector antennas are typically installed with a fixed or (mechanically / electrically) variable down-tilt in order to limit the radius/horizon of the antenna footprint and avoid excess interference with surrounding cells.

VSWR
The Voltage Standing Wave Ratio indicates how well the antenna is matched to the coaxial cable, and how much of the to-be-transmitted radio signal is actually converted to radio waves versus reflected back on the RF cable towards the transmitter. An ideal antenna has a VSWR of 1 (sometimes written 1:1). Real antennas are typically in the range of 1.2 to 2.

Side Lobes
A directional antenna never radiates only in one direction but always has certain side lobes pointing outside of the main direction of the antenna. The number and strength of side lobes differ from antenna to antenna model.

Note
Whenever installing antennas it is important to understand that any metallic or otherwise conductive object in their vicinity will inevitably alter the antenna performance. This can affect the radiation pattern, but also de-tune the antenna and shift its frequency band outside the nominal usable frequency band. It is thus best to mount antennas as far as practically possible from conductive elements within their radiation pattern

11.7.1 Omni-directional Antennas

Omni-directional antennas are typically thin long dipole antennas covered with fiberglass. They radiate with equal strength in all directions and thus result in a more or less circular cell footprint (assuming flat terrain). The shape of the radiation pattern is a torus (donut) with the antenna located in the center of that torus.

Omni-directional antennas come with a variety of gains, typically from 0 dBd to 3 dBd, 6 dBd and sometimes 9 dBd. This gain is achieved by compressing the radiation torus in the vertical plane.

Sometimes, Omni-directional antennas can be obtained with a fixed down-tilt to limit the cell radius.

11.7.2 Sector Antennas

Sector antennas are used in sectorized cell setups. Sector antennas can have significantly higher gain than omni-directional antennas.

Instead of mounting a single BTS with an omni-directional antenna to a given antenna pole, multiple BTSs with each one sector antenna are mounted to the same pole. This results in an overall larger radius due to the higher gain of the sector antennas, and also in an overall capacity increase, as each sector has the same capacity as a single omni-directional cell. And all that benefit still requires only a single physical site with antenna pole, power supply, back-haul cabling, etc.

Experimentation and simulation has shown that typically the use of three sectors with antennas of an opening angle of 65 degrees results in the most optimal combination for GSM networks. If more sectors are being deployed, there is a lot of overlap between the sectors, and the amount of hand-overs between the BTSs is increased.

11.8 RF Low Noise Amplifier (LNA)

A RF Low Noise Amplifier (LNA) is a device that amplifies the weak received signal. In general, LNAs are combined with band filters, to ensure that only those frequencies within the receive band are amplified, and out-of-band interferers are filtered out. A duplexer can already be a sufficient band-filter, depending on its characteristics.

The use of a LNA typically only makes sense if you . have very long and/or lossy coaxial cables from your antenna to the BTS, and . can mount the duplexer + LNA close to the antenna, so that the amplification happens before the long/lossy coaxial line to the BTS

Key characteristics of a LNA are:

Frequency range
A LNA is typically designed for a specific frequency range. Only signals inside that range will be properly amplified

Gain in dB
This tells you how many dB the low noise amplifier will increase your signal. `Pout = Pin + Gain`

Maximum Input Power
This indicates the maximum RF power at the PA input before saturation.

Noise Figure
This indicates how much noise this LNA will add to the signal. This noise will add to the interference as seen by the receiver.

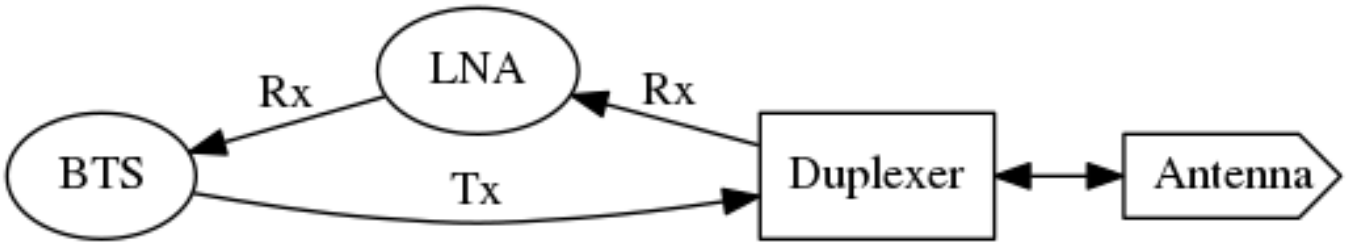


Figure 23: Addition of a RF Low Noise Amplifier to the GSM BTS Setup

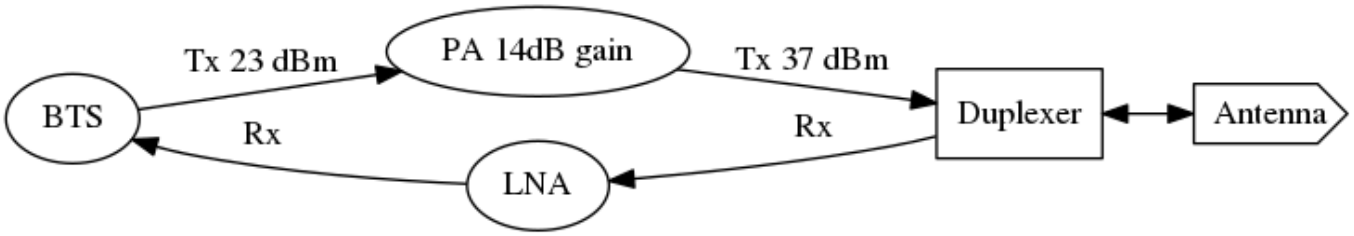


Figure 24: Addition of a RF LNA + RF PA to the GSM BTS Setup

As any LNA will add noise to the signal, it is generally discouraged to add them to the system. Instead, we recommend you to mount the entire BTS closer to the antenna, thereby removing the losses created by lengthy coaxial wire. The power supply lines and Ethernet connection to the BTS are far less critical when it comes to cable length.

12 Introduction into GSM Radio Planning

The main focus of the manual you are reading is to document the specifics of the Osmocom GSM implementation in terms of configuration, system administration and monitoring. That's basically all on the software part.

However, successful deployment and operation of GSM networks depends to a large extent on the proper design on the radio frequency (RF) side, including the right cabling, duplexers, antennas, etc.

Planning and implementing GSM deployment is a science (or art) in itself, and in most cases it is best to consult with somebody who has existing experience in the field.

There are three parts to this:

GSM Radio Network Planning
: This includes an analysis of the coverage area, its terrain/geography, the selection of the right sites for your BTSs, the antenna height, a path loss estimate. As a result of that process, it will be clear what amount of transmit power, antenna gain, cable length/type, etc. you should use to obtain the intended coverage.

GSM Site Installation
: This is the execution of what has been determined in the previous step. The required skills are quite different, as this is about properly assembling RF cables and connections, duplexers, power amplifiers, antennas, etc.

Coverage testing
: This is typically done by driving or walking in the newly-deployed GSM site, and checking of the coverage is as it was expected.

Note
This chapter can only give you the briefest overview about the process used, and cannot replace the experience and skill of somebody with GSM RF planning and site deployment.

12.1 GSM Radio Network Planning

In GSM Radio Network Planning, the number and location of sites as well as type of required equipment is determined based on the coverage requirements.

For the coverage of a single BTS, this is a process that takes into consideration:

- the terrain that needs to be covered
- the type of mobile stations to be supported, and particularly the speed of their movement (residential, pedestrians, trains, highways)
- the possible locations for cell sites, where BTSs and Antennas can be placed, as well as the possible antenna mounting height
- the equipment choices available, including
  - type and capabilities of BTS. The key criteria here is the downlink transmit power in dBm, and the uplink receive sensitivity.
  - antenna models, including gain, radiation pattern, etc.
  - RF cabling, including the key aspect of attenuation per length
  - RF duplexers, splitting the transmit and receive path
  - power amplifiers (PAs), increasing the transmit power
  - low noise amplifiers (LNAs), amplifying the received signal

For coverage of an actual cellular network consisting of neighboring cells, this process also must take into consideration aspects of *frequency planning*, which is the allocation of frequencies (ARFCNs) to the individual cells within the network. As part of that, interference generated by frequency re-use of other (distant) cells must be taken into consideration. The details of this would go beyond this very introductory text. There is plenty of literature on this subject available.

12.2 The Decibel (dB) and Decibel-Milliwatt (dBm)

RF engineering heavily depends on the Decibel (dB) as a unit to express attenuation (losses) or amplification (gain) impacted on radio signals.

The dB is a logarithmic unit, it is used to express the ratio of two values of physical quantity. You can thus not express an absolute value in dB, only relative.

Note
Relative loss (cable, connector, duplexer, splitter) **or gain** (amplifiers) are power **is expressed in dB**.

In order to express an absolute value, you need to use a unit like *dBm*, which is referencing a power of 1 mW (milli-Watt).

Note
Absolute power like transmitter output power or receiver input power **is expressed in dBm**.

Table 8: Example table of dBm values and their corresponding RF Power

dBm	RF Power	Comment
0	1 mW	
1	1.26 mW	transmit power of sysmoBTS 1002 when used with `max_power_red 22`
3	2 mW	
6	4 mW	
12	16 mW	
12	16 mW	

Table 8: (continued)

dBm	RF Power	Comment
20	100 mW	
23	199 mW	Maximum transmit power of indoor sysmoBTS 1002
26	398 mW	
30	1 W	Maximum transmit power of a MS in 1800/1900 MHz band
33	2 W	Maximum transmit power of a MS in 850/900 MHz band
37	5 W	Maximum transmit power of 1 TRX in sysmoBTS 2050
40	10 W	Maximum transmit power of sysmoBTS 1100

12.3 GSM Frequency Bands

GSM can operate in a variety of frequency bands. However, internationally only the following four bands have been deployed in actual networks:

Table 9: Table of GSM Frequency Bands

Name	Uplink Band	Downlink Band	ARFCN Range
GSM 850	824 MHz .. 849 MHz	869 MHz .. 894 MHz	128 .. 251
E-GSM 900	880 MHz .. 915 MHz	925 MHz .. 960 MHz	0 .. 124, 975 .. 1023
DCS 1800	1710 MHz .. 1785 MHz	1805 MHz .. 1880 MHz	512 .. 885
PCS 1900	1850 MHz .. 1910 MHz	1930 MHz .. 1990 MHz	512 .. 810

12.4 Path Loss

A fundamental concept in planning any type of radio communications link is the concept of *Path Loss*. Path Loss describes the amount of signal loss (attenuation) between a receive and a transmitter.

As GSM operates in frequency duplex on uplink and downlink, there is correspondingly an *Uplink Path Loss* from MS to BTS, and a *Downlink Path Loss* from BTS to MS. Both need to be considered.

It is possible to compute the path loss in a theoretical ideal situation, where transmitter and receiver are in empty space, with no surfaces anywhere nearby causing reflections, and with no objects or materials in between them. This is generally called the *Free Space Path Loss*.

Estimating the path loss within a given real-world terrain/geography is a hard problem, and there are no easy solutions. It is impacted, among other things, by

- the height of the transmitter and receiver antennas
- whether there is line-of-sight (LOS) or non-line-of-sight (NLOS)
- the geography/terrain in terms of hills, mountains, etc.
- the vegetation in terms of attenuation by foliage
- any type of construction, and if so, the type of materials used in that construction, the height of the buildings, their distance, etc.
- the frequency (band) used. Lower frequencies generally expose better NLOS characteristics than higher frequencies.

The above factors determine on the one hand side the actual attenuation of the radio wave between transmitter and receiver. On the other hand, they also determine how many reflections there are on this path, causing so-called *Multipath Fading* of the signal.

Over decades, many different radio propagation models have been designed by scientists and engineers. They might be based on empirical studies condensed down into relatively simple models, or they might be based on ray-tracing in a 3D model of the terrain.

Several companies have developed (expensive, proprietary) simulation software that can help with this process in detail. However, the results of such simulation also depend significantly on the availability of precise 3D models of the geography/terrain as well as the building structure in the coverage area.

In absence of such simulation software and/or precise models, there are several models that can help, depending on the general terrain:

Table 10: List of common path loss models

Type	Sub-Type	Bands	Name
Terrain	-	850, 900, 1800, 1900	ITU terrain model
Rural	Foliage	850, 900, 1800, 1900	One woodland terminal model
City	Urban	850, 900	Okumura-Hata Model for Urban Areas
City	Suburban	850, 900	Okumura-Hata Model for Suburban Areas
City	Open	850, 900	Okumura-Hata Model for Open Areas
City	Urban	1800, 1900	COST-231 Hata Model
Indoor	-	900, 1800, 1900	ITU model for indoor attenuation

In Table 10 you can see a list of commonly-used path loss models. They are typically quite simple equations which only require certain parameters like the distance of transmitter and receiver as well as the antenna height, etc. No detailed 3D models of the terrain are required.

FIXME: Example calculations

12.5 Link Budget

The link budget consists of the total budget of all elements in the telecommunication system between BTS and MS (and vice-versa).

This includes

- antenna gains on both sides
- coaxial cabling between antenna and receiver/transmitter
- losses in duplexers, splitters, connectors, etc
- gain of any amplifiers (PA, LNA)
- path loss of the radio link between the two antennas

The simplified link budget equations looks like this:

```
Rx Power (dBm) = Tx Power (dBm) + Gains (dB) - Losses (dB)
```

Gains is the sum of all gains, including

- Gain of the transmitter antenna
- Gain of the receiver antenna

- Gain of any PA (transmitter) or LNA (receiver)

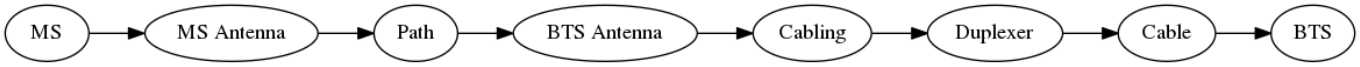
Losses is the sum of all losses, including

- Loss of any cabling and/or connectors on either side
- Loss of any passive components like duplexers/splitters on either side
- Path Loss of the radio link

Using the Link Budget equation and resolving it for the path loss will give you an idea of how much path loss on the radio link you can afford while still having a reliable radio link. Resolving the path loss into a physical distance based on your path loss model will then give you an idea about the coverage area that you can expect.

The Rx Power substituted in the Link budget equation is determined by the receiver sensitivity. It is customary to add some some safety margin to cover for fading.

12.5.1 Uplink Link Budget



The transmit power of a MS depends on various factors, such as the MS Power Class, the frequency band and the modulation scheme used.

Table 11: Typical MS transmit power levels

Power Class	Band	Modulation	Power
4	850 / 900	GMSK	33 dBm (2 W)
1	1800 / 1900	GMSK	30 dBm (1 W)
E2	850 / 900	8PSK	27 dBm (0.5 W)
E2	1800 / 1900	8PSK	26 dBm (0.4 W)

The minimum reference sensitivity level of a normal GSM BTS is specified in 3GPP TS 05.05 and required to be at least -104 dBm. Most modern BTSs outperform this significantly.

FIXME: Example calculation (spreadsheet screenshot?)

12.5.2 Downlink Link Budget

The transmit power of the BTS depends on your BTS model and any possible external power amplifiers used.

The minimum reference sensitivity level of a GSM MS is specified in 3GPP TS 05.05 and can typically be assumed to be about -102 dB.

FIXME: Example calculation (spreadsheet screenshot?)

12.5.3 Optimization of the Link Budget

If the coverage area determined by the above procedure is insufficient, you can try to change some of the parameters, such as

- increasing transmit power by adding a bigger PA
- increasing antenna gain by using a higher gain antenna
- reducing cable losses by using better / shorter coaxial cables
- increasing the height of your antenna == Osmocom SS7 + SIGTRAN support

12.6 History / Background

If you're upgrading from earlier releases of the Osmocom stack, this section will give you some background about the evolution.

12.6.1 The Past (before 2017)

In the original implementation of the GSM BSC inside Osmocom (the OsmoBSC program, part of OpenBSC), no SS7 support was included.

This is despite the fact that ETSI/3GPP mandated the use of SCCP over MTP over E1/T1 TDM lines for the A interface at that time.

Instead of going down to the TDM based legacy physical layers, OsmoBSC implemented someting called an IPA multiplex, which apparently some people also refer to as SCCPlite. We have never seen any specifications for this interface, but implemented it from scratch using protocol traces.

The IPA protocol stack is based on a minimal sub-set of SCCP (including connection oriented SCCP) wrapped into a 3-byte header to packetize a TCP stream.

The IPA/SCCPlite based A interface existed at a time when the ETSI/3GPP specifications did not offer any IP based transport for the A interface. An official as added only in Release FIXME of the 3GPP specifications.

The A interface BSSMAP protocol refers to voice circuits (E1/T1 timeslots) using circuit identity codes (CICs). As there are no physical timeslots on a TCP/IP based transport layer, the CICs get mapped to RTP streams for circuit-switched data using out-of-band signaling via MGCP, the IETF-standardized Media Gateway Control Protocol.

12.6.2 The present (2017)

In 2017, sysmocom was tasked with implementing a 3GPP AoIP compliant A interface. This meant that lot of things had to change in the existing code:

- removal of the existing hard-wired SCCPlite/IPA code from OsmoBSC
- introduction of a formal SCCP User SAP at the lower boundary of BSSMAP
- introduction of libosmo-sigtran, a comprehensive SS7 and SIGTRAN library which includes a SCCP implementation for connectionless and connection-oriented procedures, offering the SCCP User SAP towards BSSAP
- introduction of an A interface in OsmoMSC (which so far offered Iu only)
- port of the existing SUA-baesd IuCS and IuPS over to the SCCP User SAP of libosmo-sigtran.
- Implementation of ETSI M3UA as preferred/primary transport layer for SCCP
- Implementation of an IPA transport layer inside libosmo-sigtran, in order to keep backwards-compatibility.

This work enables the Osmocom universe to become more compliant with modern Releases of 3GPP specifications, which enables interoperability with other MSCs or even BSCs. However, this comes at a price: Increased complexity in set-up and configuration.

Using SS7 or SIGTRAN based transport of the A interface adds an entirely new domain that needs to be understood by system and network administrators setting up cellular networks based on Osmocom.

One of the key advantages of the Osmocom architecture with OsmoNITB was exactly this simplification and reduction of complexity, enabling more people to set-up and operate cellular networks.

So we have put some thought into how we can achieve compatibility with SS7/SIGTRAN and the 3GPP specifications, while at the same time enabling some degree of auto-configuration where a small network can be set up without too many configuration related to the signaling network. We have achieved this by "abusing" (or extending) the M3UA Routing Key Management slightly.

12.7 Osmocom extensions to SIGTRAN

Osmocom has implemented some extensions to the SIGTRAN protocol suite. Those extensions will be documented below.

12.7.1 Osmocom M3UA Routing Key Management Extensions

In classic M3UA, a peer identifies its remote peer based on IP address and port details. So once an ASP connects to an SG, the SG will check if there is any configuration that matches the source IP (and possibly source port) of that connection in order to understand which routing context is used - and subsequently which traffic is to be routed to this M3UA peer.

This is quite inflexible, as it means that every BSC in a GSM network needs to be manually pre-configured at the SG/STP, and that configuration on the BSC and MSC must match to enable communication.

M3UA specifies an optional Routing Key Management (RKM) sub-protocol. Using RKM, an ASP can dynamically tell the SG/STP, which traffic it wants to receive. However, the idea is still that the SG has some matching configuration.

In OsmoSTP based on libosmo-sigtran, we decided to (optionally) enable fully dynamic registration. This means that any ASP can simply connect to the SG and request the dynamic creation of an ASP and AS with a corresponding routing key for a given point code. As long as the SG doesn't already have a route to this requested point code, The SG will simply trust any ASP and set a corresponding route.

To enable dynamic creation of ASPs within an AS from any source IP/port, the corresponding xUA Server (Section 12.10) must be configured with `accept-asp-connections dynamic-permitted`.

To enable dynamic registration of routing keys via RKM, the corresponding SS7 Instance (Section 12.9) must be confgured with `xua rkm routing-key-allocation dynamic-permitted`.

This is of course highly insecure and can only be used in trusted, internal networks. However, it is quite elegant in reducing the amount of configuration complexity. All that is needed, is that an unique point code is configured at each of the ASPs (application programs) that connect to the STP.

To put things more concretely: Each BSC and MSC connecting to OsmoSTP simply needs to be configured to have a different point code, and to know to which IP/port of the STP to connect. There's no other configuration required for a small, autonomous, self-contained network. OsmoSTP will automatically install ASP, AS and route definitions on demand, and route messages between all connected entities.

The same above of course also applies to HNB-GW and OsmoSGSN in the case of Iu interfaces.

12.7.2 IPA / SCCPlite backwards compatibility

The fundamental problem with IPA/SCCPlite is that there's no MTP routing label surrounding the SCCP message. This is generally problematic in the context of connection-oriented SCCP, as there is no addressing information inside the SCCP messages after the connection has been established. Instead, the messages are routed based on the MTP label, containing point codes established during connection set-up time.

This means that even if the SCCP messages did contain Called/Calling Party Addresses with point codes or global titles, it would only help us for routing connectionless SCCP. The A interface, however, is connection-oriented.

So in order to integrate IPA/SCCPlite with a new full-blown SS7/SIGTRAN stack, there are the following options:

1. implement SCCP connection coupling. This is something like a proxy for connection-oriented SCCP, and is what is used in SS7 to route beyond a given MTP netwokr (e.g. at gateways between different MTP networks)

2. consider all SCCP messages to be destined for the local point code of the receiver. This then means that the SG functionality must be included inside the MSC, and the MSC be bound to the SSN on the local point code.
3. hard-code some DPC when receiving a message from an IPA connection. It could be any remote PC and we'd simply route the message towards that point code.

But then we also have the return direction:

1. We could "assign" a unique SPC to each connected IPA client (BSC), and then announce that PC towards the SS7 side. Return packets would then end up at our IPA-server-bearing STP, which forwards them to the respective IPA connection and thus BSC. On the transmit side, we'd simply strip the MTP routing label and send the raw SCCP message over IPA.
2. If the IPA server / SGW resides within the MSC, one could also have some kind of handle/reference to the specific TCP connection through which the BSC connected. All responses for a given peer would then have to be routed back to the same connection. This is quite ugly as it completely breaks the concepts of the SCCP User SAP, where a user has no information (nor to worry about) any "physical" signaling links.

12.8 Minimal Osmocom SIGTRAN configurations for small networks

If you're not an SS7 expert, and all you want is to run your own small self-contained cellular network, this section explains what you need to do.

In general, you can consider OsmoSTP as something like an IP router. On the application layer (in our case the BSSAP/BSSMAP or RANAP protocols between Radio Access Network and Core Network), it is completely invisible/transparent. The BSC connects via SCCP to the MSC. It doesn't know that there's an STP in between, and that this STP is performing some routing function. Compares this to your web browser not knowing about IP routers, it just establishes an http connection to a web server.

This is also why most GSM nework architecture diagrams will not explicitly show an STP. It is not part of the cellular network. Rather, one or many STPs are part of the underlying SS7 signaling transport network, on top of which the cellular network elements are built.

12.8.1 A minimal 2G configuration to get started

You will be running the following programs:

- OsmoBSC as the base-station controller between your BTS (possibly running OsmoBTS) and the MSC
- OsmoMSC as the mobile switching center providing SMS and telephony service to your subscribers
- OsmoSTP as the signal transfer point, routing messages between one or more BSCs and the MSC

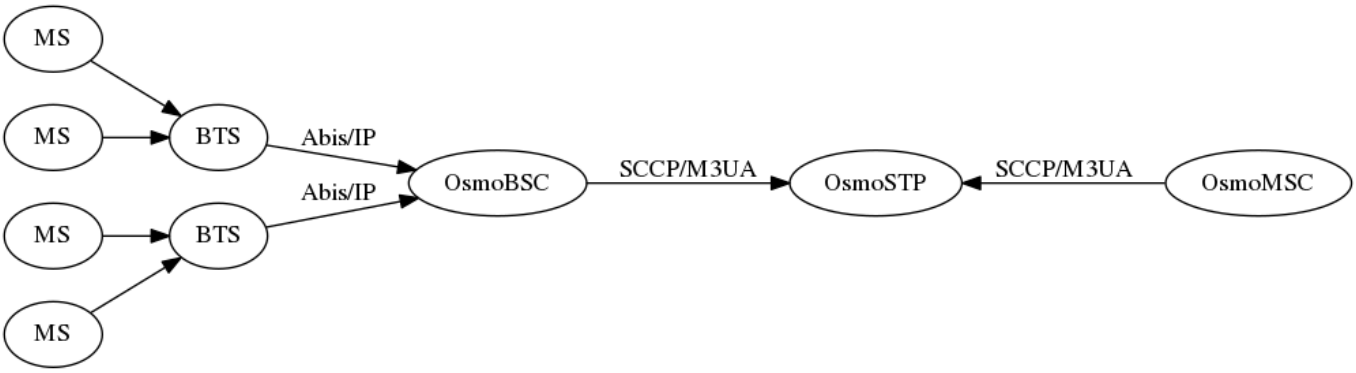


Figure 25: Simple signaling network for 2G (GSM)

You can use the OsmoSTP fully dynamic registration feature, so the BSCs and the MSC will simply register with their point codes to the STP, and the STP will create most configuration on the fly.

All you need to make sure is:

- to assign one unique point code to each BSC and MSC
- to point all BSCs and the MSC to connect to the IP+Port of the STP
- to configure the point code of the MSC in the BSCs

12.8.2 A minimaal 3G configuration to get started

You will be running the following programs:

- OsmoHNBGW as the homeNodeB Gateway between your femtocells / small cells and the MSC+SGSN
- OsmoMSC as the mobile switching center providing SMS and telephony service to your subscribers
- OsmoSGSN as the Serving GPRS Support Node, providing packet data (internet) services to your subscribers
- OsmoSTP as the signal transfer point, routing messages between one or more HNBGWs and the MSC and SGSN

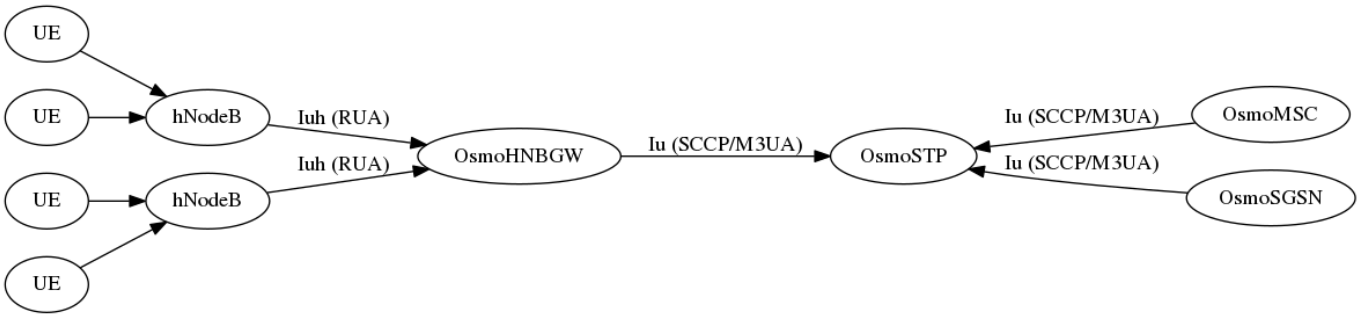


Figure 26: Simple signaling network for 3G (UMTS)

You can use the OsmoSTP fully dynamic registration feature, so the HNBGWs, the SMC and the SGSNwill simply register with their point codes to the STP, and the STP will create most configuration on the fly.

All you need to make sure is:

- to assign one unique point code to each HNBGW, MSC and SGSN
- to point all HNBGWs and the MSC and SGSN to connect to the IP+Port of STP
- to configure the point code of the MSC in the HNBGWs
- to configure the point code of the SGSN in the HNBGWs

12.9 Osmocom SS7 Instances

The entire SS7 stack can be operated multiple times within one application/program by means of so-called SS7 Instances.

There can be any number of SS7 Instances, and each instance has its own set of XUA Servers, ASPs, ASs, Routes, etc.

Each SS7 Instance can have different point code formats / lengths.

Table 12: Major Attributes of an Osmocom SS7 Instance

Name	VTY Command	Description
ID	(config)# cs7 instance ID	The numeric identifier of this instance
Name	(config-cs7)# name NAME	A human-readable name for this instance
Description	(config-cs7)# description DESC	More verbose description
Primary PC	(config-cs7)# point-code PC	Primary local point code
Network Indicator	(config-cs7)# network-indicator	Network Indicator used in MTP3 Routing Label
Point Code Format	(config-cs7)# point-code format	Point Code Format (Default: 3.8.3)
Point Code Delimiter	(config-cs7)# point-code delimiter	Point Code Delimiter: . or -

12.10 Osmocom SS7 xUA Server

A **xUA Server** is a server that binds + listens to a given SCTP (SIGTRAN) or TCP (IPA) port and accepts connections from remote peers (ASPs).

There can be any number of xUA Servers within one SS7 Instance, as long as they all run on a different combination of IP address and port.

Table 13: Major Attributes of an Osmocom SS7 xUA Server

Name	Description
Local IP	Local Port Number to which the server shall bind/listen
Local Port	Local IP Address to which the server shall bind/listen
Protocol	Protocol (M3UA, SUA, IPA) to be operated by this server
Accept Dynamic ASPs	Should we accept connections from ASPs that are not explicitly pre-configured with their source IP and port?

12.11 Osmocom SS7 Users

A SS7 User is part of a program that binds to a given MTP-Layer Service Indicator (SI). The Osmocom SS7 stack offers an API to register SS7 Users, as well as the VTY command `show cs7 instance <0-15> users` to list the currently registered users.

12.12 Osmocom SS7 Links

Conceptually, SS7 links are on the same level as SIGTRAN ASPs. The details of SS7 Links in the Osmocom implementation are TBD.

12.13 Osmocom SS7 Linksets

Conceptually, SS7 Linksets are on the same level as SIGTRAN ASs. The details of SS7 Links in the Osmocom implementation are TBD.

12.14 Osmocom SS7 Application Servers

This corresponds 1:1 to the SIGTRAN concept of an Application Server, i.e. a given external Application that interfaces the SS7 network via a SS7 protocol variant such as M3UA.

In the context of Osmocom, for each program connecting to a STP (like a BSC or MSC), you will have one Application Server definition.

An AS has the following properties:

Table 14: Major Attributes of an Osmocom SS7 Application Server

Name	Description
Name	A human-readable name for this instance
Description	More verbose description (for human user only)
Protocol	Protocol (M3UA, SUA, IPA) to be operated by this server
Routing Key	Routing Key (mostly Point Code) routed to this AS
Traffic Mode	Theoretically Bradcast, Load-Balance. Currently only Ovverride
Recovery Timeout	Duration of the AS T(r) recovery timer. During this time, outgoing messages are queued. If the AS is ACTIVE before timer expiration, the queue is drained. At expriation, the queue is flushed.
State	Application Server State (Down, Inactive, Active, Pending)
ASPs	Which ASPs are permitted to transfer traffic for this AS

12.15 Osmocom SS7 Application Server Processes

An Application Server Process corresponds to a given SCTP (or TCP) connection. From the STP/SG (Server) point-of-view, those are incoming connections from Application Servers such as the BSCs. From the ASP (Client) Point of view, it has one `osmo_ss7_asp` object for each outbound SIGTARN connection.

An ASP has the following properties:

Table 15: Major Attributes of an Osmocom SS7 Application Server Process

Name	Description
Name	A human-readable name for this instance
Description	More verbose description (for human user only)
Protocol	Protocol (M3UA, SUA, IPA) to be operated by this server
Role	Server (SG) or Client (ASP)?
Local Port	Port Number of the local end of the connection
Local IP	IP Address of the local end of the connection
Remote Port	Port Number of the remote end of the connection
Remote IP	IP Address of the remote end of the connection
State	ASP State (Down, Inactive, Active)

12.16 Osmocom SS7 Routes

An Osmocom SS7 Route routes traffic with a matching destination point code and point code mask (similar to IP Address + Netmask) towards a specified SS7 Linkset or Application Server. The Linkset or Application Servers are identified by their name.

Table 16: Major Attributes of an Osmocom SS7 Application Server Process

Name	Description
Point Code	Destination Point Code for this route
Mask	Destination Mask for this route (like an IP netmask)
Linkset/AS Name	Destination Linkset or AS, identified by name

12.17 Osmocom SCCP Instances

An Osmocom SS7 Instance can be bound to an Osmocom SS7 Instance. It will register/bind for the ITU-standard Service Indicator (SI).

12.18 Osmocom SCCP User

An Program (like a BSC) will *bind* itself to a given well-known sub-system number (SSN) in order to receive SCCP messages destined for this SSN.

There is an API to bind a program to a SSN, which implicitly generates an SCCP User object.

The `show cs7 instance <0-15> sccp users` command can be used on the VTY to obtain a list of currently bound SCCP users, as well as their corresponding SSNs.

12.19 Osmocom SCCP Connection

This is how Osmocom represents each individual connection of connection-oriented SCCP.

To illustrate the practical applicaiton: For the common use case of the A or Iu interfaces, this means that every dedicated radio channel that is currently active to any UE/MS has one SCCP connection to the MSC and/or SGSN.

The `show cs7 instance <0-15> sccp connections` command can be used on the VTY to obtain a list of currently active SCCP connections, as well as their source/destination and current state.

12.20 Osmocom SCCP User SAP

The Osmocom SCCP User SAP (Service Access Point) is the programming interface between the SCCP Provider (libosmo-sigtran) and the SCCP User (such as osmo-bsc, osmo-msc, osmo-hnbgw, etc.). It follows primitives as laid out in [itu-t-q711], encapsulated in `osmo_prim` structures.

12.21 Osmocom MTP User SAP

The Osmocom MTP User SAP (Service Access Point) is the programming interface between the MTP Provider and the MTP User (e.g. SCCP). It follows primitives as laid out in [itu-t-q711], encapsulated in `osmo_prim` structures. == Signaling Networks: SS7 and SIGTRAN

Classic digital telephony networks (whether wired or wireless) use the ITU-T SS7 (Signaling System 7) to exchange signaling information between network elements.

Most of the ETSI/3GPP interfaces in the GSM and UMTS network are also based on top of [parts of] SS7. This includes, among others, the following interfaces:

- *A* interface between BSC and MSC
- *IuCS* interface between RNC (or HNB-GW) and MSC

- *IuPS* interface between RNC (or HNB-GW) and SGSN

Note
This does not include the A-bis interface between BTS and BSC. While Abis traditionally is spoken over the same physical TDM circuits as SS7, the protocol stack from L2 upwards is quite different (Abis uses LAPD, while SS7 uses MTP)!

12.22 Physical Layer

The traditional physical layer of SS7 is based on TDM (time division multiplex) links of the PDH/SDH family, as they were common in ISDN networks. Some people may know their smallest incarnation as so-called E1/T1 links. It can run either on individual 64kBps timeslots of such a link, or on entire 2Mbps/1.5MBps E1/T1 links.

There are also specifications for SS7 over ATM, though it is unclear to the author if this is actually still used anywhere.

On top of the Physical Layer is the Message Transfer Part (MTP).

12.23 Message Transfer Part (MTP)

MTP is the lower layer of the SS7 protocol stack. It is comprised of two sub-layes, called MTP2 and MTP3.

Nodes in a MTP network are addressed by their unique PC (Point Code).

A *MTP Routing Label* is in the MTP header and indicates the *Originationg Point Code* (OPC) as well as the *Destination Point Code* (DPC) and the *Service Indicator Octet* (SIO). The SIO is used to de-multiplex between different upper-layer protocol such as ISUP, TUP or SCCP.

Routing is performed by means of routers with routing tables, similar to routing is performed in IP networks. Even the concept of a *point code mask* analogous to the *netmask* exists.

Routers are connected with one another over one or more *Link Sets*, each comprised of one or multiple *Links*. Multiple Links in a Linkset exist both for load sharing as well as for fail over purposes.

12.23.1 Point Codes

The length of point codes depends on the particular MTP dialect that is used. In the 1980ies, when international telephony signaling networks were established, most countries had their own national dialects with certain specifics.

Today, mostly the ITU and ANSI variants survive. The ITU variant uses 14bit point codes, while the ANSI variant uses 24 bit point code length.

Point Codes can be represented either as unsigned integers, or grouped. Unfortunately there is no standard as to their representation. In ITU networks, the *3.8.3* notation is commonly used, i.e. one decimal for the first 3 bits, followed by one decimal for the center 8 bits, followed by another decimal for the final 3 bits.

Example
The Point Code **1.5.3** (in 3.8.3 notation) is $1*2^{11} + 5*2^3 + 3$ = **2091 decimal**.

12.24 Higher-Layer Protocols

There are various higher-layer protocols used on top of MTP3, such as TUP, ISUP, BICC as well as SCCP. Those protocols exist side-by-side on top of MTP3, similar to e.g. ICMP, TCP and UDP existing side-by-side on top of IP.

In the context of cellular networks, SCCP is the most relevant part.

12.25 Signaling Connection Control Part (SCCP)

SCCP runs on top of MTP3 and creates something like an overlay network on top of it. SCCP communication can e.g. span multiple different isolated MTP networks, each with their own MTP dialect and addressing.

SCCP provides both connectionless (datagram) and connection-oriented services. Both are used in the context of cellular networks.

12.25.1 SCCP Adresses

SCCP Adresses are quite complex. This is due to the fact that it is not simply one address format, but in fact a choice of one or multiple different types of addresses.

SCCP Addresses exist as *Calling Party* and *Called Party* addresses. In the context of connectionless datagram services, the sender is always the Calling Party, and the receiver the Called Party. In connection-oriented SCCP, they resemble the initiator and recipient of the connection.

Table 17: SCCP Address Parts

Acronym	Name	Description
SSN	Sub-System Number	Describes a given application such as e.g. a GSM MSC, BSC or HLR. Can be compared to port numbers on the Internet
PC	Point Code	The Point Code of the underlying MTP network
GT	Global Title	What most people would call a "phone number". However, Global Titles come in many different numbering plans, and only one of them (E.164) resembles actual phone numbers.
RI	Routing Indicator	Determines if message shall be routed on PC+SSN or on GT basis

12.25.2 Global Titles

A Global Title is a (typically) globally unique address in the global telephony network. The body of the Global Title consists of a series of BCD-encoded digits similar to what everyone knows as phone numbers.

A GT is however not only the digits of the "phone number", but also some other equally important information, such as the *Numbering Plan* as well as the *Nature of Address Indication*.

Table 18: Global Title Parts

Acronym	Name	Description
GTI	Global Title Indicator	Determines the GT Format. Ranges from no GT (0) to GT+TT+NP+ES+NAI (4)
NAI	Nature of Address Indicator	Exists in GTI=1 and is sort of a mixture of TON + NPI
TT	Translation Type	Used as a look-up key in Global Title Translation Tables
NP	Numbering Plan	Indicates ITU Numbering Plan, such as E.164, E.212, E.214
ES	Encoding Scheme	Just a peculiar way to idicate the length of the digits
-	Signals	The actual "phone number digits"

For more information about SCCP Adresses and Global Titles, please refer to [itu-t-q713]

12.25.3 Global Title Translation (GTT)

Global Title Translation is a process of re-writing the Global Title on-the-fly while a signaling message passes a STP.

Basically, a SCCP message is first transported by MTP3 on the MTP level to the Destination Point Code indicated in the MTP Routing Label. This process uses MTP routing and is transparent to SCCP.

Once the SCCP message arrives at the MTP End-Node identified by the Destination Point Code, the message is handed up to the local SCCP stack, which then may implement Global Title Translation.

The input to the GTT process is

- the destination address of the SCCP message
- a local list/database of Global Title Translation Rules

The successful output of he GTT includes

- A new Routing Indicator
- The Destination Point Code to which the message is forwarded on MTP level
- a Sub-system Number (if RI is set to "Route on SSN")
- a new Global Title (if RI is set to "Route on GT"), e.g. with translated digits.

Between sender and recipient of a signaling message, there can be many instances of Global Title Translation (up to 15 as per the hop counter).

For more information on Global Title Translation, please refer to [itu-t-q714].

12.25.4 Peculiarities of Connection Oriented SCCP

Interestingly, Connection-Oriented SCCP messages carry SCCP Addresses **only during connection establishment**. All data messages during an ongoing connection do not contain a Called or Calling Party Address. Instead, they are routed only by the MTP label, which is constructed from point code information saved at the time the connection is established.

This means that connection-oriented SCCP can not be routed across MTP network boundaries the same way as connectionless SCCP messages. Instead, an STP would have to perform *connection coupling*, whic is basically the equivalent of an application-level proxy between two SCCP connections, each over one of the two MTP networks.

This is probably mostly of theoretical relevance, as connection-oriented SCCP is primarily used between RAN and CN of cellular network inside one operator, i.e. not across multiple MTP networks.

12.26 SIGTRAN - SS7 over IP Networks

At some point, IP based networks became more dominant than classic ISDN networks, and 3GPP as well as IETF were working out methods in which telecom signaling traffic can be adapted over IP based networks.

Initially, only the edge of the network (i.e. the applications talking to the network, such as HLR or MSC) were attached to the existing old SS7 backbone by means as SUA and M3UA. Over time, even the links of the actual network backbone networks became more and more IP based.

In order to replace existing TDM-based SS7 links/liksets with SIGTRAN, the M2UA or M2PA variants are used as a kind of drop-in replacement for physical links.

All SIGTRAN share that while they use IP, they don't use TCP or UDP but operate over a (then) newly-introduced Layer 4 transport protocol on top of IP: SCTP (Stream Control Transmission Protocol).

Despite first being specified in October 2000 as IETF RFC 2960, it took a long time until solid implementations of SCTP ended up in general-purpose operating systems. SCTP is not used much outside the context of SIGTAN, which means implementations often suffer from bugs, and many parts of the public Internet do not carry SCTP traffic due to restrictive firewalls and/or ignorant network administrators.

12.26.1 SIGTRAN Concepts / Terminology

Like every protocol or technology, SIGTRAN brings with it its own terminology and concepts. This section tries to briefly introduce them. For more information, please see the related IETF RFCs.

12.26.1.1 Signaling Gateway (SG)

The Signaling Gateway (SG) interconnects the SS7 network wit external applications. It translates (parts of) the SS7 protocol stack into an IP based SIGTRAN protocol stack. Which parts at which level of the protocol stack are translated to what depends on the specific SIGTRAN dialect.

A SG is traditionally attached to the TDM-Based SS7 network and offers SIGTRAN/IP based applications a way to remotely attach to the SS7 network.

A SG typically has STP functionality built-in, but it is not mandatory.

12.26.1.2 Application Server (AS)

An Application Server is basically a logical entity representing one particular external application (from the SS7 point of view) which is interfaced with the SS7 network by means of one of the SIGTRAN protocols.

An Application Server can have one or more Application Server Processes associated with it. This functionality (currently not implemented in Osmocom) can be used for load-balancing or fail-over scenarios.

12.26.1.3 Application Server Process (ASP)

An Application Server Process represents one particular SCTP connection used for SIGTRAN signaling between an external application (e.g. a BSC) and the Signaling Gateway (SG).

One Application Server Process can route traffic for multiple Application Servers. In order to differentiate traffic for different Application Servers, the Routing Context header is used.

12.26.2 SIGTRAN variants / stackings

SIGTRAN is the name of an IETF working group, which has released an entire group of different protocol specifications. So rather than one way of transporting classic telecom signaling over IP, there are now half a dozen different ones, and all can claim to be an official IETF standard.

FIXME: Overview picture comparing the different stackings

12.26.2.1 MTP3 User Adaptation (M3UA)

M3UA basically "chops off" everything up to and including the MTP3 protocol layer of the SS7 protocol stack and replaces it with a stack comprised of M3UA over SCTP over IP.

M3UA is specified in [ietf-rfc4666].

12.26.2.2 SCCP User Adaptation (SUA)

SUA basically "chops off" everything up to and including the SCCP protocol layer of the SS7 protocol stack and replaces it with a stack comprised of SUA over SCTP over IP.

This means that SUA can only be used for SCCP based signaling, but not for other SS7 protocols like e.g. TUP and ISUP.

SUA is specified in [ietf-rfc3868].

12.26.2.3 MTP2 User Adaptation (M2UA)

M2UA is specified in [ietf-rfc3331].

Note
M2UA is not supported in Osmocom SIGTRAN up to this point. Let us know if we can implement it for you!

12.26.2.4 MTP2-User Peer-to-Peer Adaptation (M2PA)

M2PA is specified in [ietf-rfc4165].

Note
M2PA is not supported in Osmocom SIGTRAN up to this point. Let us know if we can implement it for you!

12.26.3 SIGTRAN security

There simply is none. There are some hints that TLS shall be used over SCTP in order to provide authenticity and/or confidentiality for SIGTRAN, but this is not widely used.

As telecom signaling is not generally carried over public networks, private networks/links by means of MPLS, VLANs or VPNs such as IPsec are often used to isolate and/or secure SIGTRAN.

Under no circumstances should you use unsecured SIGTRAN with production data over the public internet!

12.26.4 IPv6 support

SCTP (and thus all the higher layer protocols of the various SIGTRAN stackings) operates on top of both IPv4 and IPv6. As the entire underlying IP transport is transparent to the SS7/SCCP applications, there is no restriction on whether to use SIGTRAN over IPv4 or IPv6.

13 Short Message Peer to Peer (SMPP)

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

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

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

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

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

13.1 Global SMPP configuration

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

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

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

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

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

13.2 ESME configuration

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

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

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

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

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

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

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

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

13.3 Example configuration snippet

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

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

13.4 Osmocom SMPP protocol extensions

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

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

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

13.4.1 RF channel measuremets

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

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

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

13.4.2 Equipment IMEI

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

TLV	IEI	Length	Purpose
TLVID_osmo_imei	0x2306	variable	IMEI of the subscibers phone (ME)

14 Regulatory Requirements

14.1 Spectrum License Required

GSM operates in licensed frequency spectrum. As a result you may not operate a BTS without having obtained a license from the regulatory authority in the country you want to operate the BTS in.

Failure to acquire a proper spectrum license or failure to comply with the terms of the license can lead to interference with public communications networks, which not only may cause civil claims by the operator of the interfered network, but is punishable as a crime under most jurisdictions.

sysmocom disclaims any responsibility for illegal / unlicensed use of its products.

14.2 Regulatory authorities by country

The following (by far incomplete) list gives you some indication of the regulatory authorities for the respective country. sysmocom does not guarantee correctness of this information.

Table 19: Regulatory authorities

Country	Name
Austria	RTR
Belgium	IBPT
Germany	Bundesnetzagentur
Italy	AGCOM
Netherlands	Agentschap Telecom
Sweden	PTS
Switzerland	Bakom
United Kingdom	Ofcom
United States of America	FCC

A more complete list of regulatory authorities including links to their web pages can be found at https://en.wikipedia.org/wiki/-List_of_telecommunications_regulatory_bodies

15 TRX Manager UDP socket interface

This is the protocol used between `osmo-trx` and `osmo-bts-trx`.

Each TRX Manager UDP socket interface represents a single ARFCN. Each of these per-ARFCN interfaces is a pair of UDP sockets, one for control and one for data. Given a base port B (5700), the master clock interface is at port P=B. The TRX-side control interface for C(N) is on port P=B+2N+1 and the data interface is on an odd numbered port P=B+2N+2. The corresponding core-side interface for every socket is at P+100. For any given build, the number of ARFCN interfaces can be fixed.

15.1 Indications on the Master Clock Interface

The master clock interface is output only (from the radio). Messages are "indications".

CLOCK gives the current value of the transceiver clock to be used by the core. This message is sent whenever a trasmission packet arrives that is too late or too early. The clock value is NOT the current transceiver time. It is a time setting the the core should use to give better packet arrival times.

```
IND CLOCK <totalFrames>
```

15.2 Commands on the Per-ARFCN Control Interface

The per-ARFCN control interface uses a command-reponse protocol. Commands are NULL-terminated ASCII strings, one per UDP socket. Each command has a corresponding response.

Every command is of the form:

```
CMD <cmdtype> [params]
```

The `<cmdtype>` is the actual command. Parameters are optional depending on the commands type. Every response is of the form:

```
RSP <cmdtype> <status> [result]
```

The `<status>` is 0 for success and a non-zero error code for failure. Successful responses may include results, depending on the command type.

15.2.1 Power Control

`POWEROFF` shuts off transmitter power and stops the demodulator.

```
CMD POWEROFF
RSP POWEROFF <status>
```

`POWERON` starts the transmitter and starts the demodulator. Initial power level is very low. This command fails if the transmitter and receiver are not yet tuned. This command fails if the transmit or receive frequency creates a conflict with another ARFCN that is already running. If the transceiver is already on, it response with success to this command.

```
CMD POWERON
RSP POWERON <status>
```

`SETPOWER` sets output power in dB wrt full scale. This command fails if the transmitter and receiver are not running.


```
CMD SETPOWER <dB>
RSP SETPOWER <status> <dB>
```

ADJPOWER adjusts power by the given dB step. Response returns resulting power level wrt full scale. This command fails if the transmitter and receiver are not running.

```
CMD ADJPOWER <dBStep>
RSP ADJPOWER <status> <dBLevel>
```

15.2.2 Tuning Control

RXTUNE tunes the receiver to a given frequency in kHz. This command fails if the receiver is already running. (To re-tune you stop the radio, re-tune, and restart.) This command fails if the transmit or receive frequency creates a conflict with another ARFCN that is already running.

```
CMD RXTUNE <kHz>
RSP RXTUNE <status> <kHz>
```

TXTUNE tunes the transmitter to a given frequency in kHz. This command fails if the transmitter is already running. (To re-tune you stop the radio, re-tune, and restart.) This command fails if the transmit or receive frequency creates a conflict with another ARFCN that is already running.

```
CMD TXTUNE <kHz>
RSP TXTUNE <status> <kHz>
```

15.2.3 Timeslot Control

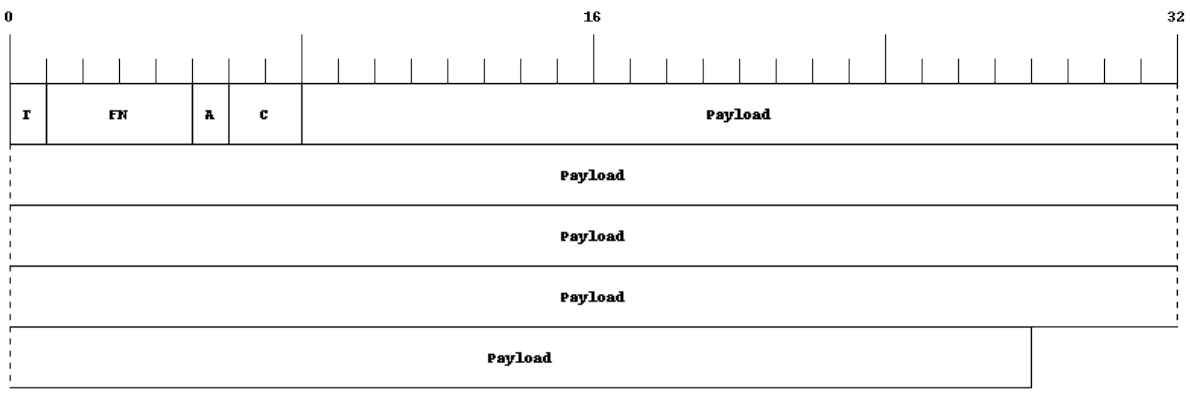
SETSLOT sets the format of the uplink timeslots in the ARFCN. The <timeslot> indicates the timeslot of interest. The <chantype> indicates the type of channel that occupies the timeslot. A chantype of zero indicates the timeslot is off.

```
CMD SETSLOT <timeslot> <chantype>
RSP SETSLOT <status> <timeslot> <chantype>
```

15.3 Messages on the per-ARFCN Data Interface

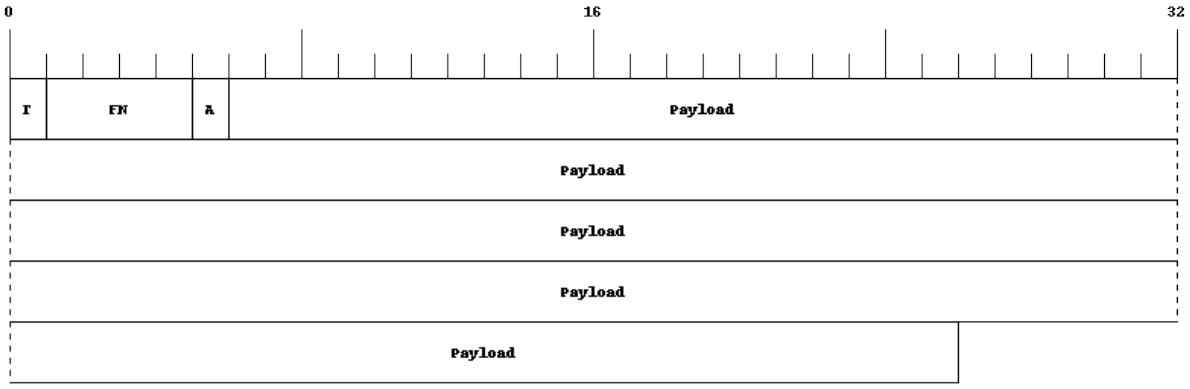
Messages on the data interface carry one radio burst per UDP message.

15.3.1 Received Data Burst



- *T*: timeslot index
- *FN*: GSM frame number, big endian
- *A*: RSSI in -dBm
- *C*: correlator timing offset in 1/256 symbol steps, 2's-comp, big endian
- *Payload*: 148 bytes soft symbol estimates, 0 → definite "0", 255 → definite "1"

15.3.2 Transmit Data Burst



- *T*: timeslot index
- *FN* GSM frame number, big endian
- *A*: transmit level wrt ARFCN max, -dB (attenuation)
- *Payload*: 148 bytes output symbol values, 0 & 1

16 The Osmocom VTY Interface

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

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

The interactive telnet VTY is used to

- explore the current status of the system, including its configuration parameters, but also to view run-time state and statistics,
- review the currently active (running) configuration,
- perform interactive changes to the configuration (for those items that do not require a program restart),
- store the current running configuration to the config file,

- enable or disable logging; to the VTY itself or to other targets.

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

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

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

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

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

Table 20: VTY Parameter Patterns

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

16.1 Accessing the telnet VTY

The VTY of a given Osmocom program is implemented as a telnet server, listening to a specific TCP port.

Please see Appendix C 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.

16.2 VTY Nodes

The VTY by default has the following minimal nodes:

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

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

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

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

16.3 Interactive help

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

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

16.3.1 The question-mark (?) command

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

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

Example: Typing ? at start of 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 Type `?` here at the prompt, the `?` itself will not be printed.

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

Example: Typing ? after a partial command

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

You may pick the `network` object and type `?` 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 without any remaining arguments being available, and that you should hit enter, a.k.a. "carriage return".

16.3.2 TAB completion

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

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

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

❶ Type `<tab>` here.

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

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

```
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 Type `<tab>` here.

16.3.3 The `list` command

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

Example: Typing list at start of 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, its software version and the current node you're at. Compare the above example of the OsmoNITB *VIEW* node with the list of 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>
```

A Bibliography / References

A.0.0.0.1 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-osmomsc] Osmocom Project: OsmoMSC User Manual. http://ftp.osmocom.org/docs/latest/-osmomsc-usermanual.pdf

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

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

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

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

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

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

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

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

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

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

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

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

[19] [3gpp-ts-24-007] 3GPP TS 24.007: Mobile radio interface signalling layer 3; General Aspects http://www.3gpp.org/DynaReport/24007.htm

[20] [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

[21] [3gpp-ts-31-101] 3GPP TS 31.101: UICC-terminal interface; Physical and logical characteristics http://www.3gpp.org/DynaReport/31101.htm

[22] [3gpp-ts-31-102] 3GPP TS 31.102: Characteristics of the Universal Subscriber Identity Module (USIM) application http://www.3gpp.org/DynaReport/31102.htm

[23] [3gpp-ts-31-111] 3GPP TS 31.111: Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) http://www.3gpp.org/DynaReport/31111.htm

[24] [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

[25] [3gpp-ts-31-116] 3GPP TS 31.116: Remote APDU Structure for (U)SIM Toolkit applications http://www.3gpp.org/DynaReport/31116.htm

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

[27] [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

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

[29] [3gpp-ts-44-064] 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

[30] [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

[31] [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

[32] [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

[33] [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

[34] [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

[35] [3gpp-ts-51-011] 3GPP TS 51.011: Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface

[36] [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

[37] [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

[38] [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

[39] [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

[40] [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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[56] [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

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

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

The BSC component is shared between OsmoBSC and OsmoNITB. This chapter describes some of the configuration options related to this shared BSC component.

A.1 Hand-over

A.1.1 Hand-over in GSM

Hand-over is the process of changing a MS with a currently active dedicated channel from one BTS to another BTS. As opposed to idle mode, where the MS autonomously performs cell re-selection, in dedicated mode this happens under network control.

In order to determine when to perform hand-over, and to which cells, the network requests the MS to perform measurements on a list of neighbor cell channels, which the MS then reports back to the network in the form of GSM RR *Measurement Result* messages. Those messages contain the downlink measurements as determined by the MS.

Furthermore, the BTS also performs measurements on the uplink, and communicates those by means of RSL to the BSC.

The hand-over decision is made by an algorithm that processes those measurement results and determines when to perform the hand-over.

A.1.2 Configuration of hand-over in OsmoBSC/OsmoNITB

OsmoBSC (like the internal BSC component of OsmoNITB) only support so-called intra-BSC hand-over, where the hand-over is performed between two BTSs within the same BSC.

Hand-over is enabled and configured by the use of a set of `handover` commands. Using those, you can tune the key parameters of the hand-over algorithm and adapt it to your specific environment.

Example handover configuration snippet

```
handover 1 ❶
handover window rxlev averaging 10 ❷
handover window rxqual averaging 1 ❸
handover window rxlev neighbor averaging 10 ❹
handover power budget interval 6 ❺
handover power budget hysteresis 3 ❻
handover maximum distance 9999 ❼
```

❶ Enable hand-over

❷ Set the RxLev averaging window for the serving cell to 10 measurements

❸ Set the RxQual averaging window for the serving cell to 1 measurement (no window)

❹ Set the RxLev averaging for neighbor cells to 10 measurements

❺ Check for the conditions of a power budget hand-over every 6 SACCH frames

❻ A neighbor cell must be at least 3 dB stronger than the serving cell to be considered a candidate for hand-over

❼ Perform a maximum distance hand-over if TA is larger 9999 (i.e. never)

A.2 Timer Configuration

The GSM specification specifies a variety of timers both on the network as well as on the mobile station side.

Those timers can be configured using the `timer tXXXX` command.

Table 21: Configurable Timers

node	timer	default	description
network	t3101	10	Timeout for *Immediate Assignment* (sec)
network	t3103	?	Timeout for Handover (sec)
network	t3105	40	Repetition of *Physical Information* (sec)
network	t3107	?	?
network	t3109	?	RSL SACCH deactivation timeout (sec)
network	t3111	?	RSL timeout to wait before releasing the RF channel (sec)
network	t3113	60	Time to try paging for a subscriber (sec)
network	t3115	?	?
network	t3117	?	?
network	t3119	?	?
network	t3122	10	Waiting time after *Immediate Assignment Reject*
network	t3141	?	?

A.3 Discontinuous Transmission (DTX)

GSM provides a full-duplex voice call service. However, in any civilized communication between human beings, only one of the participants is speaking at any given point in time. This means that most of the time, one of the two directions of the radio link is transmitting so-called *silence frames*.

During such periods of quiescence in one of the two directions, it is possible to suppress transmission of most of the radio bursts, as there is no voice signal to transport. GSM calls this feature *Discontinuous Transmission*. It exists separately for uplink (DTXu) and downlink (DTXd).

Downlink DTX is only permitted on non-primary transceivers (!= TRX0), as TRX0 must always transmit at constant output power to ensure it is detected during cell selection.

Uplink DTX is possible on any TRX, and serves primarily two uses:

possible on any TRX, and serves primarily two uses:

1. reducing the MS battery consumption by transmitting at a lower duty cycle
2. reducing the uplink interference caused in surrounding cells that re-use the same ARFCN.

DTS for both uplink and downlink is implemented in the BTS. Not all BTS models support it.

The Osmocom BSC component can instruct the BTS to enable or disable uplink and/or downlink DTX by means of A-bis OML.

B GNU Free Documentation License

Version 1.3, 3 November 2008

B.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.

B.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.

B.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 B.4.

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

B.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.

B.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.

B.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".

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

B.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.

C 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 22: TCP/UDP port numbers

L4 Protocol	Port Number	Purpose	Software
UDP	2427	MGCP GW	osmo-bsc_mgcp, osmo-mgw
TCP	2775	SMPP (SMS interface for external programs)	osmo-nitb
TCP	3002	A-bis/IP OML	osmo-bts, osmo-bsc, osmo-nitb
TCP	3003	A-bis/IP RSL	osmo-bts, osmo-bsc, osmo-nitb
TCP	4236	Control Interface	osmo-trx
TCP	4237	telnet (VTY)	osmo-trx
TCP	4238	Control Interface	osmo-bts
TCP	4239	telnet (VTY)	osmo-stp
TCP	4240	telnet (VTY)	osmo-pcu
TCP	4241	telnet (VTY)	osmo-bts
TCP	4242	telnet (VTY)	osmo-nitb, osmo-bsc, cellmgr-ng
TCP	4243	telnet (VTY)	osmo-bsc_mgcp, osmo-mgw
TCP	4244	telnet (VTY)	osmo-bsc_nat
TCP	4245	telnet (VTY)	osmo-sgsn
TCP	4246	telnet (VTY)	osmo-gbproxy
TCP	4247	telnet (VTY)	OsmocomBB
TCP	4249	Control Interface	osmo-nitb, osmo-bsc
TCP	4250	Control Interface	osmo-bsc_nat
TCP	4251	Control Interface	osmo-sgsn
TCP	4252	telnet (VTY)	sysmobts-mgr
TCP	4253	telnet (VTY)	osmo-gtphub
TCP	4254	telnet (VTY)	osmo-msc
TCP	4255	Control Interface	osmo-msc
TCP	4256	telnet (VTY)	osmo-sip-connector
TCP	4257	Control Interface	osmo-ggsn, ggsn (OpenGGSN)
TCP	4258	telnet (VTY)	osmo-hlr
TCP	4259	Control Interface	osmo-hlr
TCP	4260	telnet (VTY)	osmo-ggsn
TCP	4261	telnet (VTY)	osmo-hnbgw
TCP	4262	Control Interface	osmo-hnbgw
TCP	4263	Control Interface	osmo-gbproxy
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

