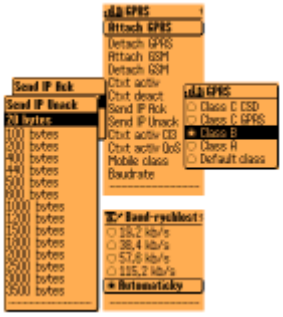
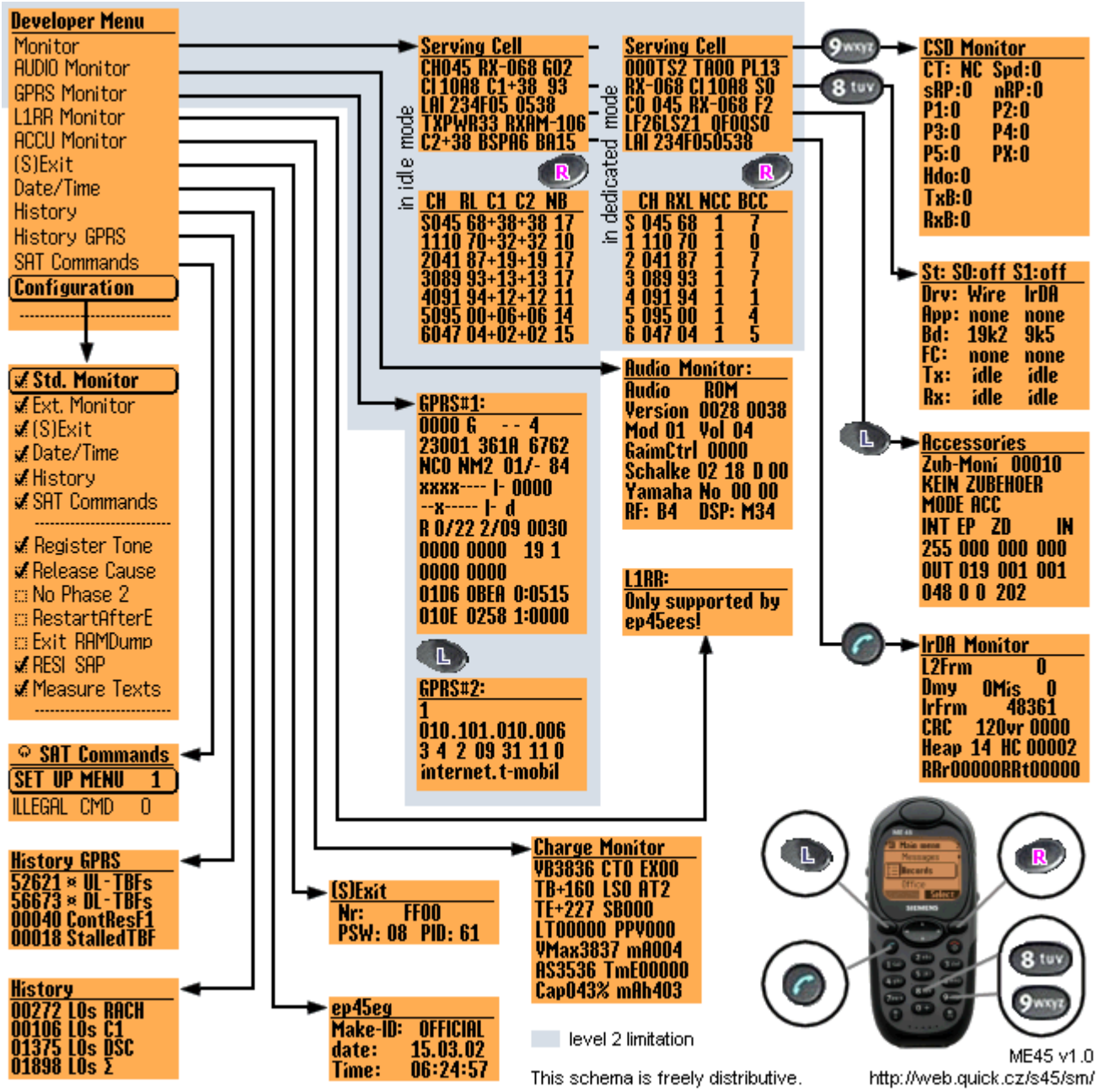
Инженерное меню Siemens S/ME45

Последние изменения: *12.08.2006*

Здесь найдете аналогичное описание SM для S45 (на чешском)



GPRS Service Menu 2



▲ Меню Monitor

Для каждой конкретной SIM-карты можно из ее кода IMSI (с помощью тщательно, но безуспешно скрываемого алгоритма) вычислить два особых "телефонных номера". Обычно вычисление производит фирма Siemens AG, однако, если Вы не желаете эту фирму беспокоить, можете использовать более быстрый и простой метод:

Скачайте и запустите свободно распространяемую программу со **страницы** одного из авторов. Огромная благодарность обоим авторам - **Greenstone & DarkBear** - можно скачать даже исходники на языке C. Если страница авторов недоступна, можно скачать **копию**, которая, конечно, может оказаться не самой последней версии.

Активация заключается в записи одного из вычесленных чисел в **последнюю** позицию телефонной книги в SIM. Имя не имеет значения (по крайней мере явно) и, зная IMSI своей карты, можно это число записать вручную, и при этом, по сути дела, не потребуется никакой кабель. Сколько бы ни было SIM-карт, для каждой из них можно вычислить числа активации.

Используя такую карту в каком-либо из многих типов телефонов Siemens **при его включении**, можно будеть вывести инженерное меню нажатием **menu** и клавиши ***** либо **#**. В зависимости от того, какое из двух чисел записано на SIM-карту, инженерное меню будет иметь различный объем.

Одно из чисел разрешает **сокращенное** инженерное меню (часть схемы, выделенная серым цветом), содержащее всего два пункта:

- **Monitor** (всего лишь отображает мониторинг сети)
- **GPRS Monitor** (всего лишь отображает мониторинг GPRS)

Другое число разрешает **полное** инженерное меню, содержащее один неизменный пункт **Configuration** и десяток других пунктов, которые можно выбрать в подменю **Configuration**.

Также существует способ активации инженерного меню, не привязанный к конкретной SIM-карте. Для этого требуется изменить несколько байтов в системной памяти телефона - установить соответствующий патч для конкретной версии прошивки. Обсуждение данного вопроса выходит за рамки статьи. С технологией установки патчей, а также с особенностями работы с различными типами флеш-памяти телефона можно ознакомиться **здесь**.

▲ Подменю Configuration

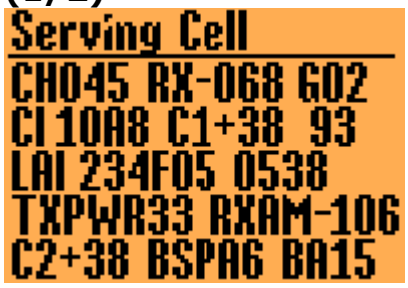
Следующие пункты **включают/выключают** отображение десяти пунктов в инженерном меню:

- **Std. Monitor**
- **Ext. Monitor**
- **(S)Exit**
- **Date/Time**
- **History**
- **SAT Commands**

Следующие пункты **включают/выключают** режимы и функции:

- **Register Tone** (звуковая индикация потери сигнала)
- **Release Cause** (cause codes CC MM RR)
- **No Phase 2**
- **Restart After Exit**
- **Exit RAM Dump** (датакабель)
- **RESI SAP** (настройка?)
- **Measure Texts**

Режим ожидания (1/2)



CH Номер частотного канала *)

RX RXLEV Reception Level, уровень приема [дБ]

G Поддержка GPRS (**-** нет поддержки), запоминается величина последнего TA (Timing Advance) с момента последнего соединения (тем не менее в режиме ожидания)

CI Cell Identity, идентификатор соты (hex)

C1 Path-loss критерий (Критерий перевыбора соты C1 [дБ])
Сколько осталось до принудительного handover (см. RX и RXAM)=RXAM-RX

xx Технологический тип SIM? (в примере 93)

LAI Local Area Identity, идентификатор области расположения абонента (в формате MCCMNC LAC)
MCC Mobile Country Code, код страны (в примере 23F4 = 324)
MNC Mobile Network Code, номер сети (в примере 05 = 50)
LAC Local Area Code, код зоны (в примере 0538)

TXPWR Allowed Transmit Power, максимально разрешенная излучаемая мощность [дБ]. Обычно 33. Бывает 30,39

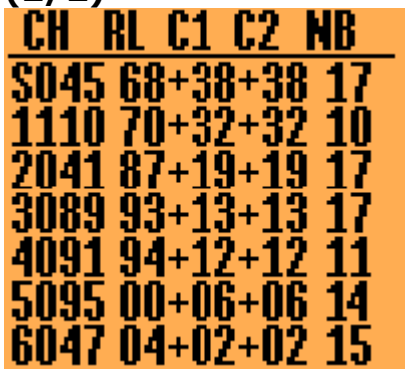
RXAM Reception Accetable Minimal Level, порог отключения приёма [дБ]

C2 Cell-reselection criterium, критерий перевыбора соты C2 [дБ]. Используется в GSM-1800 и для GSM-900 эквивалентен C1.
Важно! Для диапазона 1800 C2=C1+константа (обычно от 12 до 30). Т.е. каналу 1800 дается фора как предпочтительному каналу. Поэтому при одинаковых параметрах C1 для 900 и 1800 телефон всегда выберет 1800

BSPA Multiframe, параметр, отвечающий за частоту включения приемника телефона. Имеет значение от 2 до 9, в большинстве сетей используется multiframe=6. Чем он больше - тем чаще телефон проверяет "что там с сетью".

BA BCCH Allocation, число каналов в макросоте.

Режим ожидания (2/2)



CH Номер частотного канала *)

RL RXLEV, уровень приема [dBm]

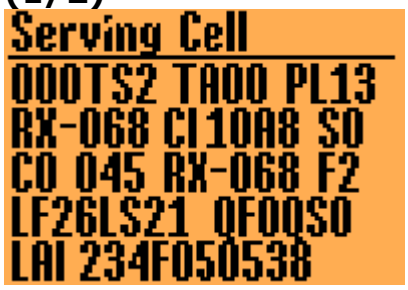
C1 Path-loss criterium

C2 Cell-reselection criterium

N NCC, National Color Code(0 - 7).
B BCC, Base Station Color Code (0 -7).
BCC отличает соты одного оператора с одинаковыми номером частотного канала, а NCC делит соты по регионам.
Эти два трехбитовых числа образуют шестибитовый BSI (Base Station Identity Code) - код идентификации базовой станции.

S Текущий канал
1 - 6 Шесть самых сильных соседних каналов

Режим разговора (1/2)



Номер текущего разговорного канала *) (000 = hopping)

TS Time Slot, канальный интервал (в канале чередуются 8 временных интервалов)

TA Timing Advance, величина временной компенсации (1 = 3,66 мкс = 547 м)
Имеет смысл расстояния до антенны.

PL Power Level, уровень мощности передатчика [PL]

RX Reception Level, уровень приема текущего разговорного канала [дБ]

CI Cell Identity, идентификатор соты (hex)

S Synchronisation burst

CO Номер текущего контрольного частотного канала *) (то же, что CH в режиме ожидания)

RX Reception Level, уровень мощности контрольного канала [дБ]

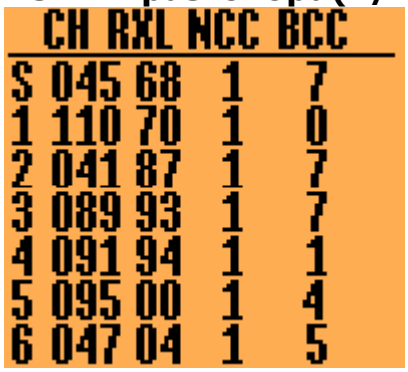
F2 Coding algorithm, используемый кодек для речи (H1=HR (HalfRate), F1=FR (FullRate), F2=EFR (Enhanced Full Rate Speech), FD=CSD data (Full Rate Data))

LF Величина C1 в случае непрерывного соединения с BTS
LS Величина C1 в случае прерывистого соединения с BTS
QF Качество связи в случае непрерывного соединения с BTS [% bit error rate]
QS Качество связи в случае прерывистого соединения с BTS [% bit error rate]

LAI Local Area Identity, идентификатор локальной зоны
MCC Mobile Country Code, код страны (в примере 23F4 = 324)
MNC Mobile Network Code, код сети (в примере 05 = 50)
LAC Local Area Code, код локальной зоны (в примере 0538)

При начале установления вызова/сервиса, когда используется канал SDCCH, на месте параметра S0 показывается используемый блок SDCCH (от 0 до 7), а на месте F2 показывается конфигурация SDCCH канала (8S или 4S, соответственно SDCCH/8 или SDCCH/4)

Режим разговора(2/2)



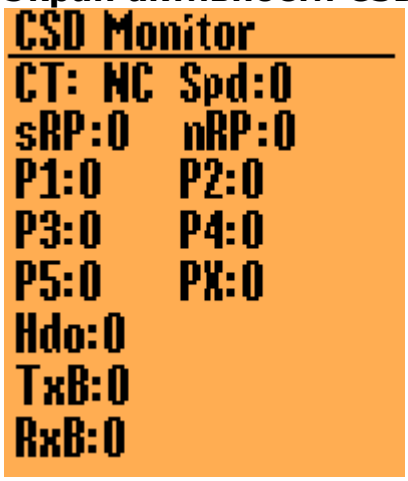
CH Номер частотного канала *)

RXL RXLEV Reception Level, уровень приема [дБ]

NCC National Color Code (0 - 7)
BCC Base Station Color Code (0 - 7)

S текущий канал
1 - 6 шесть самых сильных соседних каналов

Экран активности CSD



Монитор CSD соединения

Экран подключений

```
St: S0:off S1:off
Drv: Wire  IrDA
App: none  none
Bd:  19k2  9k5
FC:  none  none
Tx:  idle  idle
Rx:  idle  idle
```

Экран подключений по кабелю и IrDA

Список подключенных принадлежностей

```
Accessories
Zub-Moni 00010
KEIN ZUBEHOER
MODE ACC
INT EP  ZD     IN
255 000 000 000
OUT 019 001 001
048 0 0 202
```

Номер строки	Параметр	Расшифровка
1	Zubehoer-Monitor	Мониторинг дополнительного оборудования
2	Kein Zubehoer	Ничего не подключено
	Headset	Гарнитура
	Datenkabel	Датакабель
	Lader	Зарядное устройство
3	MODE ACC	Режим ожидания
	MODE DATA	Обмен данными
4	INT EP ZD	?
5	IN/OUT	?

Экран активности IrDA

```
IrDA Monitor
L2Frm        0
Dmy   0Mis   0
IrFrm     48361
CRC   120vr 0000
Heap 14 HC 00002
RRr00000RRt00000
```

Монитор IrDA

Аудиомонитор

При нажатии левой дисплейной клавиши можно задавать десятичные числа, но о их значении можно только

```
Audio Monitor:
Audio     ROM
Version 0028 0038
Mod 01  Vol 04
GaimCtrl 0000
Schalke 02 18 D 00
Yamaha No  00 00
RF: B4   DSP: M34
```

догадываться

Экран активности GPRS 1/2

```
GPRS#1:
0000 G    - - 4
23001 361A 6762
NC0 NM2 01/- 84
xxxx---- |- 0000
--x----- |- d
R 0/22 2/09 0030
0000 0000   19 1
0000 0000
01D6 0BEA 0:0515
010E 0258 1:0000
```

0000 Канал BCCH (C0)
Последний номер канала, по которому мы работали или разговаривали. Если включен хоппинг, то будет всегда 0000
G Поддержка GPRS (**-** нет поддержки)
- Канал PBCCH (в примере нет)
- PBCCH timeslot (0-7, H при хоппинге, в примере нет)
4 Priority Access (0-4)

23001 MCC/MNC
361A LAC
6762 CI (hex)

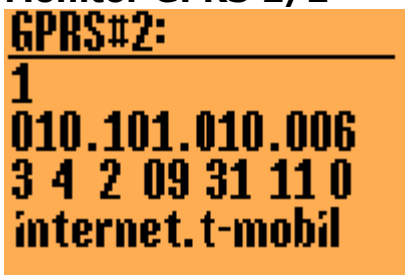
NC0 Network Control Order (0-2)
NM2 Network Mode (1-3)
01 Величина TA (0-63, **-** нет поддержки)
- Timeslot TA (0-7, в примере нет поддержки)
84 Routering Area Code - RAC (hex)

xxxx---- Тайм-слоты на прием (0-7, x - занятые)
Информация обновляется только при измемении
I Режим RLC (Radio Link Control) на прием (A - с подтверждением, U - без подтверждения, I - idle)
- Схема кодирования на прием (CS-1,2,3,4)
Каждый тайм-слот (в зависимости от схемы кодирования) способен обеспечить скорость пропускания информации от 9.05 кбит/с до 21.4 кбит/с: (схема1 - 9.05, схема2 - 13.4, схема3 - 15.6, схема4 - 21.4).
0000 Канал PBCCH (H при хоппинге)

--x----- Тайм-слоты на передачу (0-7, x - занятые)
Информация обновляется только при измемении
I Режим RLC на передачу (A - с подтверждением, U - без подтверждения, I - idle)
- Схема кодирования на передачу (CS-1,2,3,4)
d Режим MAC (F - фиксированное распределение радиоблоков, D - динамическое распределение, E - расширенное динамическое распределение)

R GMM - GPRS Mobility Management (R - ready, S - standby)
0/22 Величина времени GMM ready - единицы (0 - 2 сек, 1 - 1 мин, 2 - 6 мин., 7 - деакт.)/величина (dec)
2/09 Величина периода времени RAU (Routing Area Update) - единицы (0 - 2 сек, 1 - 1 мин, 2- 6 мин, 7 - деакт.)/величина (dec)
0 Шифрование GPRS (0 - выключено, 1 - включено)
0 Граница Gs (0 - не функционирует, 1 - функционирует)

Monitor GPRS 2/2



1 Количество PDP контекстов (отображаются только первые три)

010.101.010.006 IP адрес

3 Класс надежности QoS
4 Класс задержки QoS
2 Класс приоритета QoS
09 Пиковая пропускная способность QoS
31 Средняя пропускная способность QoS
11 LLC-SAPI (3,5,9,11)
0 0 - инициировано мобильным телефоном - MO (Mobile Originated), 1 - мобильное окончание, инициировано сотой - MT (Mobile Terminated)

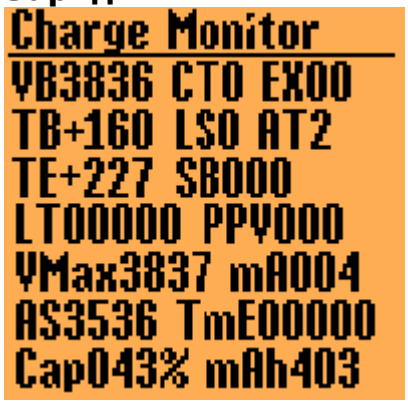
QoS (Quality of Service) Parameters

internet.t-mobil APN (11 знаков), еще может отображаться код возврата (hex)

L1RR

Совершенно непонятно, что это такое :-(

Заряд



VB Текущее напряжение на аккумуляторе xxxx [mV]
Когда стало на 1 меньше чем ASxxxx, говорит, что аккумулятор разряжен.

CT Состояние зарядного устройства
0 = не подключено
1 = подключено (контакты 1-2 замкнуты = автомобильное)
2 = подключено (контакты 1-2 разомкнуты = стандартное)

EX EXxx при работе

EX04 ближе к концу зарадки
После отключения сетевого стало 12(13)
EX00 после выключения телефона

TB Для LiIon: сопротивление между землей и средним выводом батареи, которое кодирует производителя батареи
082 = Panasonic
150 = NEC
270 = Sanyo
560 = noname
(реальная величина сопротивления немного отличается)
Для NiMH: температура аккумулятора, К

LS Статус (режим) заряда
0=рабочий режим телефона - зарядное устройство не подключено
1=капельный заряд
2=заряд номинальным током (SB100 ед., при превышении VBxxxx UMAXxxxx срабатывает термисторный предохранитель - тогда SB001 ед., EX4)
3=заряд уменьшенным током (SB085 ед.---SB001 ед., индикатор батареи на дисплее полный, EX13)
4=окончание заряда (отключение зарядного устр., обнуление LT00000, SB000, EX12)
5=рабочий режим телефона с подзарядом - зарядное устр. подключено (EX12 , LT считает с 00000, аккум. периодически подзаряжается током SB085 ед., т.е. идет поддержка VBxxxx = UMAXxxxx)

AT Производитель аккумулятора
1 = Panasonic
2 = NEC
3 = Sanyo
4 = noname
По другим данным, тип аккумулятора (1 - NiMh, 2,3 Li-Ion)

TE Окружающая температура вблизи аккумулятора xx,x [° C]

SB Индикация напряжения на 2-м контакте коннектора (с помощью которого мобильник переключает величину тока зарядки с зарядного устройства)
085 = капельный заряд (1 A)
000 = заряд номинальным током (50 - 100 mA)
По другим данным:
SB000 при работе
SB100 при зарядке
SB001 ближе к концу зарядки, когда EX стало 04

LT Таймер зарядки, увеличивающийся на 1 каждые 5 секунд

PPV Ход зарядки (ток зарядки в %?)

100 = капельный заряд (большую часть времени зарядки)
098 = незадолго до окончания капельного заряда
097 - 020 = постепенное уменьшение тока
000 = заряд номинальным током либо окончание зарядки

VMax Максимальная (пиковая) величина напряжения аккумулятора (за последние несколько секунд)

mA Текущий потребляемый ток/ток заряда [mA]

AS Величина напряжения для автоматического отключения z по причине разрядки аккумулятора. Не является константой, вычисляется с учетом текущего напряжения потребления.

TmE

Cap Оставшаяся емкость аккумулятора в % (как правило, актуализируется с большими интервалами и всегда при включении).

mAh Потребленная расчетная емкость от аккумулятора [mAh] (регулярно увеличивается, при включении пересчитывается - может и значительно измениться).

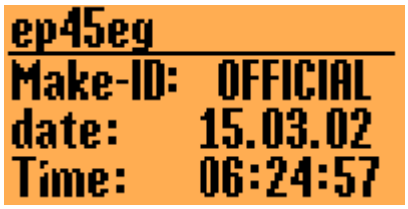
Поскольку все это крайне приблизительно, берите все с запасом. Отношения между отдельными данными слишком сложные и, очевидно, включают в себя различные зависящие от времени ограничения, когда VB>VMAX, когда в случае NiMH аккумулятора значение TB отличается от точного значения и т.д. Слишком много теории

(S)Exit

Информация о последнем неожиданном выключении, например в легендарном C35i после выключения при ошибке "Stopwatch Save Entry":
(S)Exit: FF00
PSW: 08 PID: 61
после выключения при ошибке "Audiomonitor in dedicated mode":
(S)Exit: 55B0
PSW: 58 PID: 61
после выключения при <Delete>:
(S)Exit: FFFF
PSW: FF PID: FF

Date/Time

Информация о программных модулях прошивки



History

27 счетчиков событий плюс информация SExit
Можно обнулить.

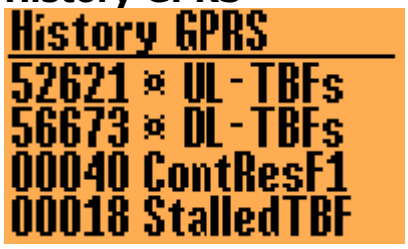
00000 LOs RACH - Logout по причине сбоя RACH
00000 LOs C1 - Logout по причине C1 < 0
00000 LOs DSC - Logout по причине DSC
00000 LOs ± - Всего Logout
00000 DSC Exp - Частота появления DSC
00001 def.Paging - Кол-во сбойных paging blocks
00011 Reselect - Кол-во перевыборов канала
00000 VAs HOFs - Потерь канала по причине сбоя во время handover
00000 VAs DSC - Потерь канала по причине истечения DSC
00000 VAs RACH - Потерь канала по причине сбоя RACH
00000 VAs SABM - Потерь канала по причине сбоя SABM
00000 VAs Ch.Rel - Потерь канала по причине неожиданного channel release
00000 HOFs no NB - Сбоев handover по причине отсутствия NB от соты
00000 HOFs No pl - Сбоев handover по причине того, что сеть не найдена
00000 HOFs SABM - Сбоев handover по причине сбоя SABM
00000 HO ± - Всего handover-ов
00000 Assignm.-F - ??? Ошибок установления соединения с сотой
00000 Assignm. S - ??? Установлений соединения с сотой
00000 BCCH-F.Ser - ??? Отказов обслуживания по контрольному каналу
00001 BCCH-F.NB - ??? Отказов по NB
00000 S VerbAufb - Кол-во всего соединений передачи данных. Голосовые вызовы (входящие и исходящие), СМС, регистрация в сети, и передача данных

0000 SEXIT
00000 S PLMNscan - Кол-во попыток поиска сети
00133 S 1B Pag. - Кол-во всех полученных пейджинговых сообщений от БС
00023 FreeTimers
65534 FreeMsgFrm
00000 User Stack
00147 S OwnPag.

DSC - (Downlink Signalling Failure Counter) Счетчик ошибок

нисходящего потока.
SABM - (Set Asynchronous Balanced Mode) Установить асинхронный симметричный режим.
RACH - (Random Access Channel) - канал параллельного доступа, используется только в направлении от подвижной станции к базовой для запроса о назначении индивидуального канала управления.
NB - (Normal Burst) С помощью этой последовательности обеспечивается: 1) оценка частоты появления ошибок в двоичных разрядах по результатам сравнения принятой и эталонной последовательностей. В процессе сравнения вычисляется параметр RXQUAL, принятый для оценки качества связи. RXQUAL используется при вхождении в связь, при выполнении процедуры "эстафетной передачи" (Handover) и при оценке зоны покрытия радиосвязью; 2) оценка импульсной характеристики радиоканала на интервале передачи NB для последующей коррекции тракта приема сигнала за счет использования адаптивного эквалайзера в тракте приема; 3) определение задержек распространения сигнала между базовой и подвижной станциями для оценки дальности связи.

History GPRS



12 счетчиков событий GPRS
Можно обнулить.

SAT Commands

Список команд SIM Application Toolkit.
Информация о выполненных командах, которыми SIM обменивается с телефоном. Пока здесь нет ничего интересного, можете поэкспериментировать с подачей команд через кабель вместо SIM, узнавая о дополнительных возможностях:

- Подавать команды AT^SSTK надо из гипертерминала (но нужно изучить кодирование)
- Nobbi's Net Monitor (подает за Вас команды по получению локальной информации)
- Шутка (подает безобидные команды **;-**)

*) *Примечание:*
GSM900 Каналы 1...124 Отображается: 1...124
E-GSM 900 Каналы 975...1023 Отображается: 125...174
GSM1800 Каналы 512...885 Отображается: 175...548
Т.е. если имеем, например, канал GSM1800, то для получения реального номера

канала надо к отображаемому значению прибавить 337: REAL_CH = CH + 337 (GSM1800)

Таблица bit error rate

QS/QF	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Величина [%]	0.2	0.4	0.8	1.6	3.2	6.4	12.8	25.6

Таблица мощности

PL	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
GSM 900 [дБ]	43	41	39	37	35	33	31	29	27	25	23	21
[Вт]	20,00	12,60	8,00	5,00	3,20	2,00	1,30	0,80	0,50	0,32	0,20	0,13
DCS 1800 [дБ]	30	28	26	24	22	20	18	16	14	12	10	8
[мВт]	1000	631	398	251	158	100	63	40	25	16	10	6,3

Максимальная мощность телефона в диапазоне GSM 900 составляет 2 Вт (PL 5), а величины PL 0 - 4 (20 Вт - 3,2 Вт) не достигаются.

Благодарность: Ivos C. и Honza K., belnetmon, DarkBear, Greenstone, GasBag, Norbert "Nobbi" Hüttisch, Janus Christian Krarup, Jazz, Ing. Martin Perný, Jan Pavelka, Skylord и другим.

Этот документ представляет собой простую компиляцию
(и попытку перевода с чешского :-))
двух наиболее полных известных мне описаний инженерного меню:
http://web.quick.cz/s45/sm/index2.html
и
http://belnetmon.bn.by/nm_siem.html

jagr