

JQ's Nokia Net Monitor Guide

Version: v0.80.1 BETA, 10/01/2004

By: Jeremy Quirke

All text and graphics © 2002-2004 Jeremy Quirke

The latest version of this document can be found at: <http://gsm.jquirke.com>

This document has been digitally signed and time-stamped to help enforce the terms and conditions listed below. The key used was my personal key:

```
pub 1024D/C321C141 2001-05-20 Jeremy Quirke
<jeremyquirke@hotmail.com>
```

```
Primary key fingerprint: 88D2 CD21 78D0 C0B7 CAEF 683A
9DF3 64E4 C321 C141
```

The time-stamping service used was Stamper. This measure has been used in order to guarantee my intellectual property rights to this document.

The document was first clear-signed with my personal key listed above, then the clear signature was submitted to Stamper where it was wrapped in Stamper's signature, to confirm the time at which the document was published.

Contents

0.1 COPYRIGHT NOTICE.....	5
0.2 FROM THE AUTHOR	5
0.3 CHANGELOG.....	6
0.4 TODO	7
0.6 STATUS.....	ERROR! BOOKMARK NOT DEFINED.
0.7 CREDITS.....	8
0.8 WHAT CAN OTHER PEOPLE DO?.....	8
0.8.1 Phones needed	8
1. WHAT IS THE NOKIA NET MONITOR?.....	9
2. WHAT CAN I DO WITH THE NOKIA NET MONITOR?	9
3. WHICH NOKIA PHONES HAVE NET MONITOR?	9
4. HOW DO I ACTIVATE NET MONITOR?	11
4.1 ENABLING NET MONITOR WITH LOGOMANAGER.....	11
4.3 FIELD TEST OR ENGINEERING?	12
4.4 CHECKING TO SEE IF NET MONITOR IS ENABLED	12
5. HOW DO I USE NET MONITOR?.....	13
5.1 WILL THE PHONE CONTINUE TO FUNCTION NORMALLY WITH NET MONITOR INFORMATION DISPLAYED?.....	14
5.2 JUMPING DIRECTLY TO TESTS.....	14
5.3 INVALID TESTS	14
5.4 VIEWING NET MONITOR INFORMATION WITH SOFTWARE	14
5.4.1 LogoManager.....	15
6. HOW DO I REMOVE NET MONITOR?	15
7. LEGALITY OF NET MONITOR	16
8. DESCRIPTION OF TECHNICAL TERMS.....	16
10. FIELD TESTS – TESTS 01 – 19	16
TEST 01 – SERVING CELL INFORMATION (1)	16
TEST 02 – SERVING CELL INFORMATION (2)	21
TEST 03 – SELECTION CHARACTERISTICS OF SERVING CELL AND NEIGHBOUR 1 AND 2	23
TEST 04 – SELECTION CHARACTERISTICS OF NEIGHBOUR 3, 4 AND 5	24
TEST 05 – SELECTION CHARACTERISTICS OF NEIGHBOUR 6, 7, AND 8	25
TEST 06 – ALLOWED AND FORBIDDEN NETWORKS	27
TEST 07 – CURRENT CELL FLAGS.....	28
TEST 08 – MULTISLOT INFORMATION	30
TEST 09 – MULTISLOT POWER OUTPUT.....	31
TEST 10 – TMSI, PRP, T3212 (LOCATION UPDATE) TIMER AND AFC/AGC INFORMATION	32
TEST 11 – CELL AND LOCAL AREA INFORMATION	33
TEST 12 – CIPHER (ENCRYPTION), HOPPING, DTX AND IMSI STATUS	34
TEST 13 – DTX MODE STATUS / TOGGLE (ACTIVE)	34
TEST 14 – CHANGE SS SCREENING INDICATOR VALUE (ACTIVE)	35
TEST 15 – MULTISLOT FRAMES INFORMATION (NOT FUNCTIONAL)	36
TEST 17 – BTS (BASE TRANSCIVER STATION) TEST (ACTIVE)	36
TEST 18 – TOGGLE BACKLIGHTS STATUS (ACTIVE).....	38
TEST 19 – CHANGE BEHAVIOUR FOR BARRED CELLS (ACTIVE).....	39
11. BATTERY/POWER TESTS – TESTS 20 – 23	41
TEST 20 – BATTERY AND CHARGING INFORMATION	41
TEST 23 – INFORMATION ABOUT BATTERY AND BATTERY USE	43
12. MISC. PHONE SOFTWARE AND STATUS INFORMATION – TESTS 30 - 39.....	43

TEST 35 – REASON FOR LAST SOFTWARE RESET	44
TEST 36 – SOFTWARE RESET STATISTICS	44
TEST 38 – MEMORY DUMP (ACTIVE)	45
TEST 39 – REASON FOR LAST CALL RELEASE	46
13. LAYER 1/LAYER 2 STATISTICS AND VARIOUS CONTROLS – TESTS 40 - 45	50
TEST 40 – RESET HANDOVER COUNTERS (ACTIVE)	50
TEST 41 – HANDOVER COUNTERS (SINGLEBAND PHONE)	50
TEST 41 – INTER-CELL HANDOVER COUNTERS (DUALBAND PHONE)	51
TEST 42 – INTRA-CELL HANDOVER COUNTERS (DUALBAND PHONE)	52
TEST 43 – LAYER 2 (DATA LINK) TIMEOUT COUNTERS	53
TEST 44 – CHANGE REVISION LEVEL (ACTIVE)	54
TEST 45 – TOGGLE TRANSMITTER ON/OFF (ACTIVE)	55
14. MEMORY AND SIM INFORMATION – TEST 51 – 57	55
TEST 51 – INFORMATION ABOUT SIM	55
TEST 54, 55 – INFORMATION ABOUT MEMORY BLOCK SETS	57
TEST 56 – INFORMATION ABOUT DOUBLE MEMORY DE-ALLOCATIONS	57
TEST 57 – STACK AND MEMORY STATUS BEFORE RESET	58
15. NETWORK RELATED STATISTICS – TEST 60 – 66	58
TEST 60 – RESET FIELD TEST COUNTERS (ACTIVE)	59
TEST 61 – SERVING CELL MEASUREMENT INFORMATION	59
TEST 61 – SERVING CELL MEASUREMENT INFORMATION (33XX)	60
TEST 62 – NEIGHBOUR MEASUREMENT INFORMATION	60
TEST 62 – NEIGHBOUR MEASUREMENT INFORMATION (33XX)	61
TEST 63 – CALL ATTEMPTS COUNTERS	62
TEST 64 – LOCATION UPDATE COUNTERS	63
TEST 65 – SMS COUNTERS	64
TEST 66 – SMS RELAY/CM LAYER COUNTERS	66
17. PHONE SOFTWARE INFORMATION – TESTS 80 – 89	67
TEST 80 – RESET TIMERS (ACTIVE)	67
TEST 81 – ENABLE/DISABLE TIMERS (ACTIVE)	68
TEST 82 – VIEW TIMERS	68
TEST 83 – CHANGE INFORMATION SHOWN IN TESTS 84-87 (ACTIVE)	69
TEST 84,85,86,87 – INFORMATION ABOUT TASKS	70
TEST 88 – INFORMATION ABOUT SOFTWARE VERSIONS	71
TEST 89 – INFORMATION ABOUT HARDWARE AND TEXT VERSION	71
18. TEST 90 AND ONWARDS	72
TEST 132 – STATISTICS ABOUT CALLS	72
19. FIELD TEST (FTD) SYMBIAN APPLICATION	73
19.1 INTRODUCTION	73
19.2 INSTALLING FTD	73
19.3 USING FTD	73
19.4 ACTIVE TESTS	74
20. FIELD TEST (FTD) – GROUP 1	75
TEST 1.1 – SERVING CELL INFORMATION (1)	75
TEST 1.2 – SERVING CELL INFORMATION (2)	76
TEST 1.3 – SELECTION CHARACTERISTICS OF SERVING CELL AND NEIGHBOUR 1 AND 2	78
TEST 1.4 – SELECTION CHARACTERISTICS OF NEIGHBOUR 3, 4 AND 5	79
TEST 1.5 – SELECTION CHARACTERISTICS OF NEIGHBOUR 6, 7, AND 8	80
TEST 1.6 – ALLOWED AND FORBIDDEN NETWORKS	82
TEST 1.7 – CURRENT CELL FLAGS	83
TEST 1.8 – TMSI, PRP, T3212 (LOCATION UPDATE) TIMER INFORMATION	84
TEST 1.9 – CELL AND LOCAL AREA INFORMATION	84
TEST 1.10 – CIPHER (ENCRYPTION), HOPPING, DTX AND IMSI STATUS	85

TEST 1.11 – DTX MODE STATUS / TOGGLE (ACTIVE)	86
TEST 1.13 – CHANGE BEHAVIOUR FOR BARRED CELLS (ACTIVE).....	87
21. FIELD TEST (FTD) – GROUP 6.....	88
TEST 6.1 – GENERAL GPRS RLC/MAC INFORMATION	88
TEST 6.2 – UPLINK TBF ESTABLISHMENT INFORMATION	90
TEST 6.3 – GMM STATE INFORMATION	91
TEST 6.4 – GMM VALUES AND NON-DRX PARAMETERS.....	93
TEST 6.5 – GPRS NETWORK PARAMETERS	94
TEST 6.6 – PCCCH PARAMETERS	96
TEST 6.7 – PACKET SYSTEM INFORMATION PARAMETERS	98
TEST 6.9 – GPRS SERVING CELL AND NEIGHBOUR INFORMATION	99
22. FIELD TEST (FTD) – GROUP 7.....	100
TEST 7.1, 7.2 – INFORMATION ABOUT ACTIVE PDP CONTEXTS	100
TEST 7.3 – RLC STATE INFORMATION.....	103
TEST 7.4 - RLC PARAMETERS	105
TEST 7.5 – RLC DATA BLOCK COUNTERS	106
TEST 7.6 – LLC DATA BLOCK COUNTERS	107
TEST 7.7 – LLC CIPHERING INFORMATION	108
TEST 7.8, 7.9 LLC PARAMETERS	108
TEST 7.10 – SNDCP DATA COUNTERS.....	110
APPENDIX A – TYPICAL AUSTRALIAN GSM NETWORK CONFIGURATIONS	111
DISCLAIMER	111
A.1 – OPTUS GSM.....	111
A.2 – TELSTRA GSM.....	116
A.3 – VODAFONE GSM	120

0.1 Copyright Notice

This document may not be modified in any way or converted into an alternate format, except in the case where software must perform an internal conversion to an internal format in order to open the document which is distributed in either Microsoft® Word 10 format or PDF format.

This document may not be printed and must remain in this electronic form as described above.

All text and graphics in this document are the work of Jeremy Quirke. Screen captures were made from various model Nokia phones, however I reserve the right to these screen captures.

If you disagree with the above terms, you must destroy this document immediately.

0.2 From the Author

Welcome to my Nokia Net Monitor Guide. I have endeavored to try and document Net Monitor to a greater extent than has ever been done before. In this document you will find detailed descriptions of many tests.

This document is by no means complete. As you will notice, there are many gaps to fill. Your continued support is much appreciated, the comments I have heard back from previous releases were quite encouraging.

I have put many hours of work into improving and updating this document as necessary. I have read and re-read differing revisions of the GSM specifications to attempt to provide the most accurate information possible. You will note many references to official specifications at the end of each paragraph in square brackets.

If you have any comments or suggestions, please email them to me. Feedback is most welcome.

To those who have helped with this document in any way, and do not see their name in the 'Credits' section, please do not take offense at my genuine mistake. Contact me immediately to rectify the situation.

I can be found:

Web: My personal website: <http://www.jquirke.com>
GSM related items (including versions of this guide):
<http://gsm.jquirke.com>

MSN: jquirke@AiBiC.net (remove 'ABC' from the address)

ICQ: 56766434

Skype: jquirke

Jabber: jquirke@jabber.org

Email: jquirke@AiBiC.net (remove 'ABC' from the address)

GSM: Contact me by the other listed means to obtain this.

- Forums: You can find me on the [Overclockers Australia](#) and [SlashDot](#) forums (to name a couple), where my username is 'jquirke'
- Usenet: I frequent (but don't necessarily post in all) alt.cellular.nokia, alt.cellular.gsm, aus.comms.mobile, aus.tv.digital (to name a few)

0.3 ChangeLog

0.80 BETA 10th January 2004

- Updated legality
- Updated list of capable phones
- Added 2100 refs
- Updated FTD general (firmware versions)
- Updated Appendix A (Telstra)
- Update from the author
- Move GSM guide stuff out
- Updated Test 03,04,05 (measurement report)
- Updated Test 07 (more Multiband information, NECI)
- Added 7110 refs
- Added Appendix A (Optus, Vodafone)
- Added Test 15
- Updated Test 2 (subtracted CROs)
- Updated FTD-6.5
- Added Test 08
- Added Test 09
- Added 6210 refs

0.75 BETA 3rd July 2003

- Added FTD-1.1
- Added FTD-1.2
- Added FTD-1.3
- Added FTD-1.4
- Added FTD-1.5
- Added FTD-1.6
- Added FTD-1.7
- Added FTD-1.8
- Added FTD-1.9
- Added FTD-1.10
- Added FTD-1.11
- Added FTD-1.13
- Added FTD-6.1
- Added FTD-6.2
- Added FTD-6.3
- Added FTD-6.4
- Added FTD-6.5
- Added FTD-6.6
- Added FTD-6.7
- Added FTD-6.9
- Added FTD-7.1
- Added FTD-7.2

- Added FTD-7.3
- Added FTD-7.4
- Added FTD-7.5
- Added FTD-7.6
- Added FTD-7.7
- Added FTD-7.8
- Added FTD-7.9
- Added FTD-7.10
- Updated Copyright, From the Author
- Updated Test 02 (nice table for page mode)
- Updated Test 13 (GSM ref)
- Added FTD general information

0.70 BETA Never officially published

- Updated Test 23 (Charge Current) [tangcla]
- Updated Test 39 (Additional causes) [tangcla]
- Updated Test 41 singleband (Max values) [Albinus]

0.65 BETA 7th February 2003

- Updated Test 01
- Updated Test 61 – 33xx
- Updated Test 62 – BCCH Ext, 33xx
- Updated Test 63 – MO calls, 33xx
- Updated Test 64 – Cause values, 33xx
- Updated Test 65 – 33xx
- Updated Test 66 – 33xx
- Added Test 39
- Added Test 44
- Updated Test 51 – Baud
- Added from author

0.6 BETA

- Added Test 43
- Updated Test 07 – added about IMSI attach/detach
- Added information about which tests in which phones
- Updated Test 19
- Updated Test 17 – added about complications on 5110 etc
- Added Test 38
- Added Test 14
- Added Test 61
- Added Test 62
- Updated Test 07 – separate samples/templates for dualb/singleb
- Fixed GSM references
- Added help screen shots
- Added Test 20
- Added Test 23
- Added Test 66
- Updated Test 65

0.5 ALPHA (2002)

- Initial distribution to friends – something to show for 2 years of experimenting with Net Monitor

0.4 TODO

- FTD-7.11, 1.12, 1.14, update 6.1, 7.7

0.6 Credits

Early stage feedback:

- Clarence 'tangcla' Tang <http://www.tangcla.com> – check out his Nokia mods

Feedback

- Albinus
- Darren Bokenham
- Kevin Baker
- Mark W

Providing phones for experimenting with:

- Clarence 'tangcla' Tang

Conversion to PDF

- Clarence Tang

Information:

* [names withheld until permission granted]

0.7 What can other people do?

- Let me borrow (maybe keep!) some phones to further investigate Net Monitor
- Anyone who has corrections LET ME KNOW! (you get credit ☺)
- Anyone who knows something I don't LET ME KNOW! (you get credit ☺)

0.7.1 Phones needed

Nokia 9xxx would be great!

1. What is the Nokia Net Monitor?

The Nokia Net Monitor is a hidden menu built into Nokia's mobile phones that allows the user to view, and in some cases change internal data about the phone's hardware, software and its connection with the mobile network. It is primarily intended for Nokia's engineers and network operators, however some interested users like to have it enabled, often "because they can".

2. What can I do with the Nokia Net Monitor?

The Nokia Net Monitor consists of a number of 'tests', each test is a page (screen) of information, some of which are interactive (explained later). Some of these tests contain useful information, others might be useless to anyone other than a Nokia engineer. In short, here is a list of some things that can be done with Net Monitor (by no means complete)

- View information about the serving cell and neighbouring cells, such as accurate signal strengths, C1 and C2 values, transmitter power, timing advance
- Lock the phone to a channel of choice, or in other words select a base station
- View information about battery capacity and charging
- Find out the reason a call terminated or couldn't be made
- Observe handover statistics
- View SMS send, receive and failure statistics
- View call statistics
- View and edit files on your SIM card (use your phone as a SIM card editor)
- Tweak audio values??
- View timers measuring the phone's uptime and how long it has been connected to a network
- View information about the SIM card
- View information about the phone's operating system
- Force the LCD and keypad backlighting on or off (useful for saving power or using phone as a torch)

3. Which Nokia phones have Net Monitor?

Until recently, all Nokia phones, even as far back as the analog phones had the Net Monitor menu, and it was relatively easy to enable on most of them.

The Nokia 2100, 3210, 3310, 3315, 3330, 3350, 5110, 5210*, 6110*, 6150*, 6210*, 6250*, 7110*, 8110, 8210*, 8250*, 8810, 8850*, 8855* and 9110 (and their various international versions) can all have Net Monitor easily enabled with a data cable and correct software. Phones marked with an asterisk ("*") can also have Net Monitor activated through an infra-red connection.

The Net Monitor menu cannot yet be enabled on the recent phones such as the Nokia 8310, 6510, 6310, 6310i, 7210, 7250, 6610. These phones are known as DCT-4 phones. The only DCT-4 phones with the Net Monitor activated are the ones that come straight from Nokia and are supplied to network operators.

The following table summarizes the methods in which Net Monitor can be enabled on various Nokia models:

Phone	Data-cable	Infra-red (IrDA/DirectIR)
2100	Yes	No
3210	Yes	No
3310	Yes	No
3315	Yes	No
3330	Yes	No
3350	Yes	No
3410	??	??
3510	??	??
3610	??	??
3650	No	No
5110	Yes	No
6100	No	No
6110	Yes	Yes
6150	Yes	Yes
6210	Yes	Yes
6250	Yes	Yes
6310	No	No
6310i	No	No
6510	No	No
6600	No	No
6610	No	No
6650	No	No
7110	Yes	Yes
7210	No	No
7250	No	No
7250i	No	No
7650*	No	No
8110	Yes	No
8210	Yes	Yes
8250	Yes	Yes
8310	No	No
8810	Yes	Unknown
8850	Yes	Yes
8855	Yes	Yes
8910	No	No
8910i	No	No
9110	Yes	No
9110i	Yes	No
9210	No	No
N-gage	No	No

*Note the 7650 can run the Ftd application, provided certain firmware requirements are met. See “Field Test (Ftd) – Symbian Application” for more information.

4. How do I activate Net Monitor?

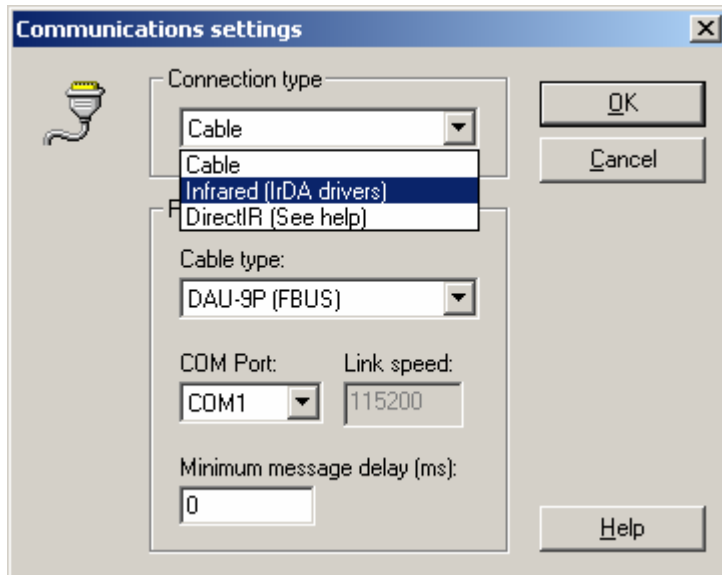
The Net Monitor menu is best enabled by connecting the phone to a PC using a data-cable or the phone’s infra-red port with software such as LogoManager.

In order to establish a connection, you will need to purchase a datacable (Link: Find out where) or use your PC’s infra-red port. The software [LogoManager](#) is recommended for Windows/Windows NT users, and the software Gnokii is recommended for *nix users (FreeBSD, Linux, etc).

If you intend to use infra-red, you will need to ensure your infra-red port is correctly detected by your operating system (this may mean having to enable it in your BIOS), and that you have turned on infra-red on your phone by selecting the “Infrared” menu in the main menu. Note if the phone does not make a connection within 2 minutes the infra-red is turned off and will need to be turned on again.

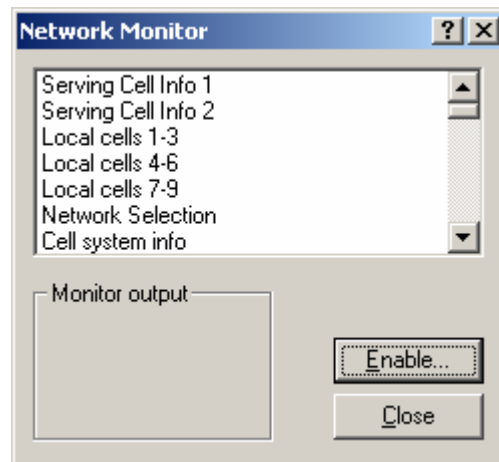
4.1 Enabling Net Monitor with LogoManager

In LogoManager you will need to ensure you have specified the correct connection type, in the Tools → Options → Change dialog.

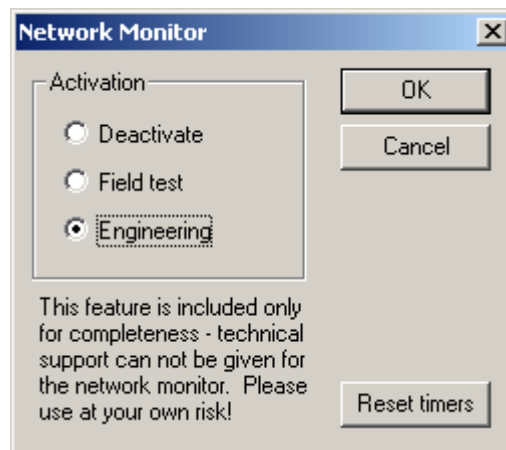


Once you have set up your connection, make sure your phone is on and LogoManager should say “Connected” in the status bar.

Once your phone has a connection, apart from transferring logos, pictures and ringtones, you can also enable Net Monitor. Select Tools → Network Monitor to bring up this dialog:



The 'Monitor output' allows you to view the Network monitor tests straight on the PC screen, see "5.4 Viewing Net Monitor with software" for more information. Click *Enable* to continue.



You then select either *Field test* or *Engineering* and click *OK* to enable Net Monitor. See the next section for more about which one to choose.

4.3 Field Test or Engineering?

Net Monitor comes in two varieties – Engineering or Field Test mode. Engineering mode offers the full functions of Net Monitor, whereas Field Test offers a cut down version of the tests generally network specific. Engineering mode includes all of the Field Test modes. You may wish to read up on individual tests to see whether you want to have the Engineering tests or not. Note it is possible to downgrade from Engineering to Field Test on the handset, but to regain the test offered by Engineering you need to use software. See "6. How do I remove Net Monitor".

4.4 Checking to see if Net Monitor is enabled

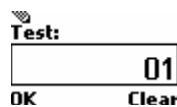
Once Net Monitor is enabled a new menu item should be present in the phone's main menu, after all of the normal menu items, that looks similar to this (varies depending on phone model – this is from my Nokia 8210):



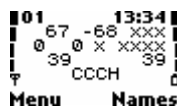
You may be curious to go into this menu but you should continue reading more of this document before doing so, as it may be possible that you can interfere with the phone's operation by randomly entering numbers.

5. How do I use Net Monitor?

Net Monitor consists of a series of tests. A test simply displays information on the home screen; sometimes this information can be changed. To get into Net Monitor, you choose the Net Monitor icon in the main menu, and a prompt will appear to enter a test number:



You then enter the number of the test you wish to view/change and press OK. For example, enter the code "01" to get test 1. Something like this should appear:



As you can see the operator logo and text areas that display profile/cell broadcasts/radio/other information have been replaced by information, that may seem meaningless. This is technical information about the phone's state and its connection with the network. You can find out more about these specific tests later in this guide.

The test number can always be seen in the top left corner of the screen. You will notice the function of the scroll keys has been changed to scrolling through the test screens – pressing down will take you to the next test (test 2 in this case) and up will take you to previous test (and will loop around to the last test in this case).

One more key that performs a function in Net Monitor is the star key. When a test is being displayed, holding the "*" key for a second or two will cause help information to be displayed. The information is not really comprehensive, it is simply a reminder as to what each value mean for those familiar with Net Monitor. Note, on some phones, such as the 8210 with recent software versions, and the 8250, the help screens will be blank, as Nokia have removed them in order to gain space for other features. To exit the help screens simply hold the "*" key again.

To clear away Net Monitor information and return the phone to its normal home screen, select test 00. This will not remove Net Monitor from the main menu, nor will it disable all of the functions Net Monitor is performing in the background or clear all

changes. To fully remove Net Monitor from the menu see (link) “6 How do I remove Net Monitor?”

5.1 Will the phone continue to function normally with Net Monitor information displayed?

Yes the phone will continue to function normally if Net Monitor is displaying information (i.e. you haven't changed anything yet). However, you won't be able to see cell broadcast information on the home screen, and on some phones you won't be able to see the caller information when you receive a phone call.

5.2 Jumping directly to tests

A couple of things to note about test numbers. Firstly, not all are valid tests, and entering the number of an invalid test will appear to do nothing, but may cause problems – see (link) “5.3 – Invalid Tests”

Another very important thing to note is that by jumping directly to valid tests, some tests interpret this as an action to perform a function for that test. These tests are active tests. For example, jumping straight to test 18 will toggle the state of the phone's keypad and LCD lights. While this is fairly harmless, other tests may alter values in the phone to make it unusable.

If you concerned about this, then it may be best to always jump to a test that is known to be a passive (non-active) test, and then scrolling to the active test from there with the scroll keys. Tests are detailed individually later in this document, and it is noted whether they are active or passive tests.

5.3 Invalid Tests

If you enter the number of an invalid test and Net Monitor is not currently being used (i.e. the home screen is normal), it will appear that nothing will happen, however if you check carefully the function the scroll keys normally perform at the home screen will no longer happen (i.e. on some phones you cannot enter the phonebook by pressing up/down or the recently dialed list). To correct this, go back to Net Monitor and select the test 00.

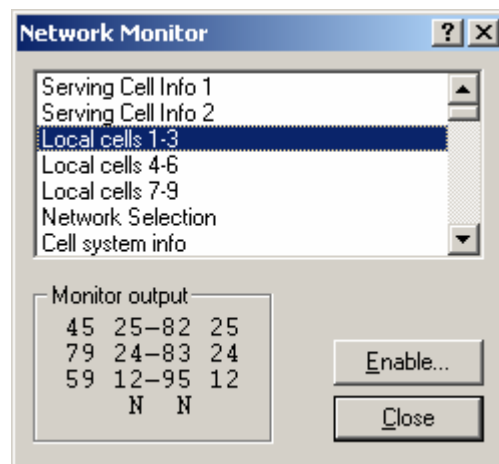
If you enter the number of an invalid test whilst Net Monitor is displaying data, the display will simply show “NO TEST” and return to the last displayed screen.

5.4 Viewing Net Monitor information with software

It is possible to observe the Net Monitor tests using software, this is useful as you can only view information and not change any settings, also some software can summarize this information, which is especially useful if you are moving and wish to take snapshots of the network conditions

5.4.1 LogoManager

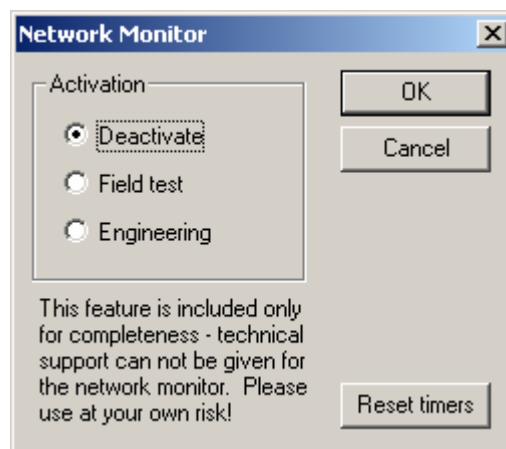
LogoManager can display the outputs of all the tests. You need to simply establish a connection with the phone, and select Tools → Network Monitor. You must have enabled Net Monitor on the phone. Then simply choose the test from the list of tests and it will be displayed in the *Monitor Output* area. Note you can view the full range of tests regardless of having Engineering or Field Test variants of Net Monitor enabled.



It is possible to use both Net Monitor on the handset and in LogoManager at the same time, viewing different tests. However, if you have toggled the help screens on the handset, the help screens will also be displayed in LogoManager.

6. How do I remove Net Monitor?

There are two ways to disable the Net Monitor menu. The first is similar to the way you enabled it – by using LogoManager or similar software and using it to disable Net Monitor – in Logo Manager, simply go *Tools* → *Network Monitor*, then click *Enable*. Select *Disable* from the list and press OK.



Alternatively, and probably more conveniently, you can disable it on the handset. Simply go to the Net Monitor menu on the handset, and enter 241 as the test number.

Once Net Monitor is disabled you cannot re-enable it again on the handset, you must use one of the (link) methods discussed before.

You can also drop the Net Monitor tests back from *Engineering* to *Field Test* by entering code 242 as the test number. This will only disable all the engineering tests (usually test 20 and above). In much the same way as disabling Net Monitor, you then cannot regain the engineering tests from the handset; you must use a PC/handheld to re-enable it.

7. Legality of Net Monitor

I am not sure how legal it is to use Net Monitor, as some functions of it allow you to override normal operating procedure defined in the GSM Specifications, tests 17 and 19 immediately come to mind, but there are others. Each jurisdiction has different telecommunications and radio regulatory bodies. I take no responsibility for what you do with Net Monitor.

8. Description of technical terms

I have moved some of the planned technical reference to the GSM standard into a separate guide, currently unreleased.

10. Field Tests – Tests 01 – 19

These tests are termed the field tests and are always present, regardless of whether “Field Test” or “Engineering” version of Net Monitor has been selected.

These tests display general parameters about the radio link with the network – signal strength, quality, information about reselection, paging, logical channels.

There are some active tests which allow the phone’s behavior to be changed – such as allowing the use of barred cells, controlling DTX mode and locking the phone to a single base station. These tests should be used with caution, after fully reading my documentation. As always, I take no responsibility with these tests.

Note, these tests can monitor other GSM networks (forbidden or not) than your own network. This is possible by using “Test 17 – BTS Test” and “Test 19 – Change Behaviour for Barred Cells”. It is also possible if you don’t use a SIM card, however you will need to use software for displaying Net Monitor tests through a data cable (infra-red cannot be enabled on most phones without a SIM).

Test 01 – Serving Cell Information (1)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about signal, selection characteristics and communication with the serving BTS. It is continued in “Test 02 – Serving Cell Information (2)”


```

01 19:46
 45 -71 xxx
 0 2 x xxxxx
 36 36
 CBCH
Menu Names

```

```

01 19:46
H 45 -73 * 5
 6 2 0 20
 34 34
 TEFR
Menu Names

```

```

01 19:46
[Colorful bars]
Menu Names

```

```

01 22:32
CH RxL TxPwr
TS TR RQ RLT
C1 CHT CZ
Menu Names

```

Red : Serving cell's radio frequency channel. In idle mode, this displays the channel of the BCCH carrier. In dedicated mode, this displays the channel the MS is using for communication. This may be preceded by a 'H' to indicate frequency hopping in dedicated mode. The display will cycle through the channels being hopped. The radio frequency channel's number also indicates what band it is in. See below. [GSM 05.05:2.x]

Light Green : Received signal strength of the serving cell in dBm. If the value is less than -100dBm, the '-' sign will not be displayed. [GSM 05.08:8.1]

Dark Blue : This value displays the output power of the transmitter. A '*' character precedes this value if the transmitter is active (which it always is if this value is displayed). If the transmitter is not active, "xxx" is displayed. [GSM 05.05:4.1.1] The meaning of the values are detailed below. ??comment on Test 45??

Yellow : The current radio timeslot. When idle, this value displays the timeslot containing the CCCH/BCCH (always 0), otherwise, in dedicated mode a value from 0-7 indicating timeslot for communication. [GSM:05.02]

Pink : The timing advance value, used by the MS to tell how early to send bursts (packets) so that they arrive in time and don't overwrite somebody else's timeslot. Units are in symbol-periods, which are 3.69 microseconds. This parameter can allow you to calculate your approximate distance to the BTS. Maximum value is 63 (35km), except for GSM400, which is 219. Since the timing advance can only be calculated after a transmission with the network, in idle mode you will need to update it by initiating a transmission, such as quickly starting a call and hanging up. [GSM:05.10]

Orange : The RXQUAL_SUB value. This value, when the phone is communicating with the BTS, shows the received signal quality, calculated from the Bit Error Rate (BER). RXQUAL_SUB differs from RXQUAL, it is used in DTX mode and calculated over a lesser number of frames. It displays 'x' when in idle mode. The RXQUAL_SUB value ranges from 0 to 7, where 0 shows the least errors (BER < 0.2%) and 7 shows the most errors (BER > 12.8%). The higher the value, the poorer quality signal and the more likely communication will fail. This value is only displayed in dedicated mode (since it only applies there). The meaning of the values is detailed below. [GSM 05.08:8.2.4]

Purple : The Radio Link Timeout value. This value controls whether the connection will be abandoned. It starts at a value assigned by the network (on BCCH), and is decreased by 1 every time an SACCH message is incorrectly decoded (corrupt), and increased by 2 every time an SACCH message is correctly decoded (intact). The

counter never exceeds the initial value, and if the counter reaches 0, the connection is terminated. The maximum initial value of the counter is 64, and the minimum is 4, and is a multiple of 4. SACCH message are sent/received usually about 2 times a second (half each 51-multiframe, which is about 235ms). This value is only displayed in dedicated mode (since it only applies there). [GSM 05.08:5.2]

Light Blue : C1 value (path loss criterion). The C1 value is calculated primarily based on signal strength, but also transmitter capability. This value is used to decide whether a cell is suitable to camp on in idle mode. It is also used in the calculation of C2 values, if supported (see “Test 07 – Current Cell Flags”). If the C1 value falls below 0, cell reselection takes place. See YYYY for more information about cell reselection. C1 value is between -99 and 999. [GSM 05.08:6.4, 6.6.2]

Dark Green : C2 value (reselection criterion). This is used to determine whether to select a new cell for camping on. If a cell’s C2 value is higher than the current cell’s C2 value for at least 5 seconds, the new cell is usually chosen. See YYYY for more information about cell reselection. If C2 values are not supported (see “Test 07 – Current Cell Flags”) or the phone is in dedicated mode, the C1 value is displayed. [GSM 05.08:6.4, 6.6.2]

Grey : The type of logical channel or sub channel or codec/data rate the phone is currently using. See below for an overview, or ZZZZ for more information. [GSM 04.03, GSM 05.02]

The GSM bands are (Tx and Rx relative to MS):

Channel	Band	Tx frequency (MHz)	Rx frequency (MHz)
1-124	GSM900, E-GSM900, R-GSM900	$890+0.2*ch$	$935+0.2*ch$
512-885	GSM1800	$1710 +0.2*(ch-511)$	$1805+0.2*(ch-511)$
975-1023	E-GSM 900,R-GSM900	$890+0.2*(ch-1023)$	$935+0.2*(ch-1023)$
0	E-GSM 900, R-GSM900	890	935
955-974	R-GSM900	$890+0.2*(ch-1023)$	$935+0.2*(ch-1023)$

It can be seen that GSM900 band is contained within E-GSM band, which in turn is contained within R-GSM band. If you are not sure which bands your phone supports you can always test them with “Test 17 – BTS Test”. If the channels are invalid, the test will display “CH: xxxx” and fail. For example, the 8210 supports GSM900, GSM1800 and E-GSM.

The Tx Power Level values are:

GSM 400, GSM850, GSM900:

Tx Power Level	Tx Power Level (dBm)
0-2	39
3	37
4	35
5	33

6	31
7	29
8	27
9	25
10	23
11	21
12	19
13	17
14	15
15	13
16	11
17	9
18	7
19-31	5

[GSM 05.05:4.1]

GSM1800:

Tx Power Level	Tx Power Level (dBm)
29	36
30	34
31	32
0	30
1	28
2	26
3	24
4	22
5	20
6	18
7	16
8	14
9	12
10	10
11	8
12	6
13	4
14	2
15-28	0

[GSM 05.05:4.1]

The RXQUAL/RXQUAL_SUB values are:

RXQUAL	Bit Error Rate (BER) (%)
0	<0.2
1	0.2 – 0.4
2	0.4 – 0.8
3	0.8 – 1.6
4	1.6 – 3.2

5	3.2 – 6.4
6	6.4 – 12.8
7	>12.8

[GSM 05.08:8.2.4]

The valid channel types are:

Channel Type	Description
CCCH	Common Control CHannel. Used for paging and allocating other channels
BCCH	Broadcast Control Channel – Used for broadcasting parameters about the network and Cell Broadcasts
CBCH	Common Control CHannel and listening for cell broadcasts on Cell Broadcast channel (downlink portion of SDCCH)
AGCH	Access Granting CHannel Sub-channel of the CCCH used for allocating other channels
SDCC	SDCCH – Standalone Dedicated Control CHannel – used for sending SMSes, location update, call setup, and other higher-layer tasks
SEAR	SEARCh – not a channel, but searching for BCCH carriers
NSPS	No Serve Power Save mode – not a channel, but sleeping temporarily as a network cannot be found
TEFR	Traffic CHannel, for voice using Enhanced Full Rate (EFR) codec
TFR	Traffic CHannel, for voice using Full Rate (FR) codec
THR0	Traffic CHannel, for voice using Half Rate (HR) codec on subchannel 0
THR1	Half Rate Traffic CHannel, for voice using Half Rate (HR) codec on subchannel 1
F144	Traffic CHannel, for data at 14.4kb/s
F96	Traffic CHannel, for data at 9.6kb/s
F72	Traffic CHannel, for data at 7.2kb/s
F48	Traffic CHannel, for data at 4.8kb/s
F24	Traffic CHannel, for data at 2.4kb/s
H480	Half Rate Traffic CHannel, for data at 4.8kb/s, subchannel 0
H481	Half Rate Traffic CHannel, for data at 4.8kb/s, subchannel 1
H240	Half Rate Traffic CHannel, for data at 2.4kb/s, subchannel 0
H241	Half Rate Traffic CHannel, for data at

	2.4kb/s, subchannel 1
FA	FACCH – Fast Associated Control Channel – subchannel of Traffic CH
FAH0	FACCH – Fast Associated Control Channel Half Rate, subchannel of Traffic CH, subchannel 0
FAH1	FACCH – Fast Associated Control Channel Half Rate, subchannel of Traffic CH, subchannel 0

Test 02 – Serving Cell Information (2)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about signal, selection characteristics and communication with the serving BTS.



Red : Paging mode. This indicates the manner in which the phone shall monitor paging and immediate assignment messages on the PCH (Paging sub-Channel of the CCCH). Values are:

Page Mode	Meaning
NO – Normal Paging	MS decodes only messages in its PCH.
EX – Extended Paging	The MS is required to decode the 2 nd PCH message from the last one.
RO – Paging Reorganisation	The MS is required to decode all messages on the CCCH and BCCH.
SB – Same as Before	The MS does not change its paging mode.

Note the MS changes its paging mode to whatever the last paging message commanded. This is why there is the SB mode, which instructs the MS to leave its paging mode as it is. [GSM 04.08:3.3.2.1.1]

Light Green : Maximum number of retransmissions allowed on the RACH when requesting a channel. RACH (Random Access Channel) is used for requesting dedicated channels. Can be 1, 2, 4, or 7. [GSM 04.08:3.3.1.1.2]

Dark Blue : Roaming Indicator. When the phone is roaming a foreign GSM network, it displays 'R'. Otherwise, it is not displayed.

Yellow : BSIC value of current cell. This value is broadcast on the SCH (in a synchronisation burst) in order to help the MS distinguish BTSs that may share the same radio channel. It is a 6-bit value, the first 3-bits are used to distinguish between carriers using the same BCCH radio channels, and the last 3-bits to distinguish between different BTSs using same BCCH radio channels. In Australia, since the carriers are guaranteed to have exclusive spectrum access, the full 6-bits can be used since there is no need to distinguish between multiple carriers sharing the same BCCH radio channel. [GSM 03.03:A.1, 05.08:7.2]

Pink : This displays the reason the last call was terminated (released). See "Test 39 – Reason for Last Call Release" for more information. [GSM 04.08:F,G,H]

Orange : The RXQUAL value. This value, when the phone is communicating with the BTS, shows the received signal quality, calculated from the Bit Error Rate (BER). It displays 'x' when in idle mode. The RXQUAL_SUB value ranges from 0 to 7, where 0 shows the least errors (BER < 0.2%) and 7 shows the most errors (BER > 12.8%). The higher the value, the poorer quality signal and the more likely communication will fail. This value is only displayed in dedicated mode (since it only applies there). The meaning of the values are detailed below. [GSM 05.08:8.2.4]

Purple : This displays the cell reselect offset (CRO), used to calculate the C2 value. It is the value added or subtracted to the C1 value. It is used to give a "weighting" to certain cells for camping. For example, Optus set it to 0 for most GSM900 cells, but micro-cells and GSM1800 cells have it set to (subtract) 20, to discourage the MS from camping on them. Ranges from 0 – 126 in steps of 2dBm. Normally this value is added to the C1 value, however, by setting the penalty time to a reserved value (31), this value is subtracted from the C1 value. Obviously, this means the temporary offset cannot be used in conjunction with a subtracted CRO. To determine if the CRO is being subtracted, normally this involves calculating the difference between C1 and C2. Additionally, if the value is being subtracted, Penalty Time will always appear as 620 seconds. This value is only displayed in idle mode, otherwise it is displayed as 'x's. [GSM 05.08:6.4]

Light Blue : This displays the temporary offset, used to calculate the C2 value. It is a value subtracted from the C1 value, like the cell reselect offset. However, it is only applied temporarily, i.e. for a certain period of time after the phone finds this cell. Then, it is removed. This is useful for cells where the MS is likely to be moving at a high enough speed such as that it will move out of range of the BTS too quickly. If the MS however is within range long enough to exceed the time period (see next section), then it can camp on the cell. Temporary offset is in steps of 10dB from 0 to 70. A value of 70dB means 'infinite', i.e. the cell cannot be used during the time period. This value is only displayed in idle mode, otherwise 'x's are shown. [GSM 05.08:6.4]

Dark Green : This displays the penalty time, which is how long the temporary offset is applied after the cell is placed on the monitoring list. After this time the temporary offset is removed when calculating the C2 value. Penalty time is in steps of 20 seconds, ranging from 0 to 620. This value is only displayed in idle mode, otherwise 'x's are shown. [GSM 05.08:6.4]

Grey : Indicates whether frequency hopping is used. Displays 1 for yes, or 0 for no. This value can only be 1 in dedicated mode. [GSM 05.02:6.2.3]

Red-Blue : MAIO – Mobile Allocation Index Offset. A value ranging from 0 to 63, this 'seeds' the phone into the hopping sequence. This allows phones to be sharing the

same timeslot and radio channels by hopping to different frequencies at different times. This value is displayed as 'x's when hopping is off.[GSM 05.02:6.2.2]

Green-Yellow : HSN – Hopping Sequence Number, a 6-bit value ranging from 0 to 63, this also is used in the calculation of the hopping sequence. If the value is 0, cyclic hopping is used (where the mobile steps through the assigned channels in sequence from the first to the last and back to the first). This value is displayed as 'x's when hopping is off. [GSM 05.02:6.2.2]

Test 03 – Selection characteristics of Serving Cell and Neighbour 1 and 2

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays a selection summary of the serving cell, and the 1st and 2nd neighbour cells.



Each cell is allocated it's own line in the display. The format of each line is identical.

Red : The radio channel number (ARFCN) of the serving cell. This will be submitted in the measurement report. See “Test 1 – Serving Cell Information (1)”. [GSM 05.05:2.x]

Light Green : The C1 value of the serving cell in idle mode. See “Test 1 – Serving Cell Information (1)”. [GSM 05.08:6.4] In dedicated mode, the BSIC value used to distinguish between multiple cells using the same channel is shown, in the form of a 2-digit value from 0-63 preceded by a 'B' (this will be submitted in the measurement report). See “Test 2 – Serving Cell Information (2)”. [GSM 03.03:A.1, 05.08:7.2]

Dark Blue : The received signal strength of the serving cell. This value is in dBm, but if the value is -100dBm or less, in order to fit the 3 digits, the '-' sign is not shown. In dedicated mode, this value will be used to calculate the RXLEV submitted in the measurement report. [GSM 05.08:8.1]

Yellow : The C2 value of the serving cell in idle mode. See “Test 1 – Serving Cell Information (1)”. If C2 values are not supported (see “Test 07 – Current Cell Flags”), the C1 value is displayed. Even if C2 values are supported, the C2 on many cells will equal the C1 value. In dedicated mode (i.e. call), the information here is meaningless (in particular for neighbour cells, since the MS may not have received the cell reselection criteria to calculate the C1/C2 values). [GSM 05.08:6.4]

Pink: A summary of information about the 1st neighbour cell, or, in dedicated mode, the information that will be used in the 1st position of the measurement report. The format is exactly the same as the serving cell information (see above).

Orange : A summary of information about the 2nd neighbour cell , or, in dedicated mode, the information that will be used in the 2nd position of the measurement report. The format is exactly the same as the serving cell information (see above).

Purple : This indicates whether the 1st neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Light Blue : This indicates the selection priority of the 1st neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Dark Green : This indicates whether the 2nd neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Grey : This indicates the selection priority of the 2nd neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Please note the 1st and 2nd neighbour cell lines may not be displayed, if there are no neighbours found to be measured, or the BTS Test (“Test 17 – BTS Test”) is enabled. Any line not displayed is shown as ‘x’s, including it’s corresponding priority and forbidden indicator. The first line (serving cell) will always be displayed, if there is no coverage on the home network, it will show information about another network. If there are no networks found, it will show the last stored values from when a network was found.

These tests (3-5) are useful for seeing the number of cells detected in the area, as well as the contents of the measurement report in dedicated mode. The measurement report is sent by the MS to the network in order for the network to make decisions for handover. To find out more information about a cell, “Test 17 – BTS Test” can be used to lock the phone to it’s channel.

With the priority indicator, normal cells are compared first, followed by low priority cells if a suitable normal cell cannot be found. Barred cells are cells which the network operator does not want phones to camp on – it might be a cell currently being tested, or for other reasons. It is possible however to use barred cells with Net Monitor, with “Test 19 – Change Behaviour for Barred Cells”. [GSM 05.08:9.table1a, 03.22:3.5.1,3.5.2]

[GSM 05.08:6.2, 6.3, 6.4, 6.6, 7.1, 7.2, 8.2, 8.4 03.22:3.x, 4.x]

Test 04 – Selection characteristics of Neighbour 3, 4 and 5

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays a selection summary of the serving cell, and the 3rd, 4th and 5th neighbour cells.

```
04      22:46
43  18-33 13
59  17-30 17
76  13-34 13
T   N   N   N   0
Menu  Names
```



```

04 22:49
47B23-91-99
59B08-93-14
43B0-96-11
N N N
Menu Names

```

```

04 22:46
[Red bar]
[Light Green bar]
[Dark Blue bar]
[Yellow bar]
[Orange bar]
[Purple bar]
[Light Blue bar]
[Dark Green bar]
Menu Names

```

```

04 22:48
SCH C1 FX C2
4CH C1 FX C2
5CH C1 FX C2
3N 4N 5N
Menu Names

```

Each cell has its own line. The format of each line is exactly the same as that of the serving cell (see “Test 3 – Selection characteristics of Serving Cell and Neighbour 1 and 2”).

Red : A summary of information about the 3rd neighbour cell, or, in dedicated mode, the information that will be used in the 3rd position of the measurement report.

Light Green : A summary of information about the 4th neighbour cell, or, in dedicated mode, the information that will be used in the 4th position of the measurement report.

Dark Blue : A summary of information about the 5th neighbour cell, or, in dedicated mode, the information that will be used in the 5th position of the measurement report.

Yellow : This indicates whether the 3rd neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Pink : This indicates the selection priority of the 3rd neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Orange : This indicates whether the 4th neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Purple : This indicates the selection priority of the 4th neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Light Blue : This indicates whether the 5th neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Dark Green : This indicates the selection priority of the 5th neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

These lines may not be displayed, if there are not enough cells to fill them, or if the BTS Test is enabled. Any line not displayed is shown as ‘x’s, including it’s corresponding priority and forbidden indicator. See Test 3 for more information.

Test 05 – Selection characteristics of Neighbour 6, 7, and 8

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays a selection summary of the serving cell, and the 6th, 7th and 8th neighbour cells.

```

05      23:10
83 10-97 10
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
  XX XX XX
Menu    Names

```

```

05      23:49
53B 6-93-99
83B43-99-99
77B 6,103-99
  N  N  N
Menu    Names

```

```

05      23:10
XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX
  XX XX XX
Menu    Names

```

```

05      22:48
6CH C1 FX C2
7CH C1 FX C2
8CH C1 FX C2
  6N 7N 8N
Menu    Names

```

Each cell has its own line. The format of each line is exactly the same as that of the serving cell (see “Test 3 – Selection characteristics of Serving Cell and Neighbour 1 and 2”).

Red : A summary of information about the 6th neighbour cell, or, in dedicated mode, the information that will be used in the 6th position of the measurement report.

Light Green : A summary of information about the 7th neighbour cell. **Dark Blue** : A summary of information about the 8th neighbour cell.

Yellow : This indicates whether the 6th neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Pink : This indicates the selection priority of the 6th neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Orange : This indicates whether the 7th neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Purple : This indicates the selection priority of the 7th neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Light Blue : This indicates whether the 8th neighbour cell is in a forbidden location. It displays ‘F’ if it is, otherwise it displays nothing.

Dark Green : This indicates the selection priority of the 8th neighbour cell. Can be ‘N’ (normal), ‘L’ (low), ‘B’ (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

These lines may not be displayed, if there are not enough cells to fill them, or if the BTS Test is enabled. Any line not displayed is shown as ‘x’s, including it’s corresponding priority and forbidden indicator. Additionally, most Nokia models do not monitor the 7th and 8th neighbour cells in idle mode, as the GSM specifications only require 6 neighbour cells to be monitored. However in dedicated mode they may display information about neighbouring cells the MS is monitoring. Also, it seems on some phone models, such as 8210, priority is not displayed for the 6th neighbour in idle mode. In my example, this is the case. See Test 3 for more information.

Test 06 – Allowed and Forbidden Networks

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about the networks you are allowed to use (or are preferred when roaming is enabled) and forbidden to use. It displays the last registered network and up to 3 preferred networks, and up to 4 forbidden networks, in the 5-digit form (3 digit Country Code, 2 digit Network Code), except for GSM1900 phones (see below). Empty fields are filled with 'x'.

06	15:10
50502	50501
52503	50503
45501	50508
45400	xxxxxx
Menu	Names

06	15:10
█	█
█	█
█	█
█	█
█	█
Menu	Names

06	23:05
L_Reg	1_For
1_Pre	2_For
2_Pre	3_For
3_Pre	4_For
Menu	Names

Red : Last GSM Network the phone successfully registered to.

Green : First preferred alternate network.

Dark Blue : Second preferred alternate network.

Yellow : Third preferred alternate network

Pink : Forbidden network 1

Orange : Forbidden network 2

Purple: Forbidden network 3

Light Blue: Forbidden network 4

Note for GSM1900 phones, the fields are 6 digits (3 digit Country Code, 3 digit Network Code).

In my example, the last registered network was my home network, 505-02 (Australia/Singtel-Optus). The three preferred networks are 525-03 (Singapore/MobileOne), 455-01 (Macau/Telemovel+), 454-00 (Hong Kong/CSL).

The forbidden networks that the MS is not allowed to use are 505-01 (Australia/Telstra MobileNet), 505-03 (Australia/Vodafone) and 505-08 (Australia/One.Tel). This list is built up when the MS tries to location update (includes IMSI-attach) to a GSM network and is rejected due to "PLMN not allowed" error. If the list is already full, the 1st entry is deleted, the rest are moved up and the new entry is stored in position 4. [GSM 04.08:4.4.4.7, 11.11:10.3.16]

The preferred networks are the networks the MS shall attempt to access in order of descending priority. [GSM 11.11:10.3.4]

This information is stored in the SIM card.

Test 07 – Current Cell Flags

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays values about the network and current cell, obtained from the current BTS.

```
(dualband)          (singleband)
07 16:15            07 16:18
E A H C I BR      E A H C I BR
1 1 0 1 0 10     1 1 0 1 0 10
ECSC 2Ter MB      Menu
1 1 0             0

07 16:15            07 16:18
E A H C I BR      E A H C I BR
1 1 0 1 0 10     1 1 0 1 0 10
ECSC 2Ter MB      Menu
1 1 0             0

07 23:18
Serving Cell
system info
bits
Menu Names
```

Note the lower half of the display only appears on dualband phones.

Red : The network allows emergency calls through 112 are possible, regardless of authentication – this information is broadcast in System Information Type 1, 2, 2bis messages. (1=Yes, 2=No)

Light Green : The IMSI-attach-detach procedure is to be used. (1=Yes, 2=No) IMSI-attach is where the phone sends a special location update to the network when it is powered up (or returns to the coverage area) (under certain conditions) to inform the network it is ready to take calls. IMSI-detach is where the phone informs the network it is not available to take calls (i.e. it may be turning off). It is like a logon/logoff, so the network doesn't bother trying to search for the phone and the caller immediately gets your voicemail or not available message. This information is broadcast in System Information Type 3 messages. [GSM 04.08:4.3.4, 4.4.3]

Dark Blue: The value of the NECI bit. The NECI bit decides whether the Phase 2 MS shall use the new establishment cause values (8-bit values) when sending a CHANNEL REQUEST on the RACH. The new establishment causes provide the network with more information about what the MS intends to do with the connection. Phase 1 networks always have the NECI bit set to 0. Most of the new establishment causes are related to TCH/H (half-rate) channel requests, this is why this field is labelled as "Half Rate Support". (1=Yes, 2=No) [GSM 04.08:9.1.8]

Yellow : C2 values are supported by the network (1=Yes, 2=No) [GSM 05.08:6.4]

Pink: System Information Messages 7 and 8 are broadcast by the cell (1=Yes, 2=No). System information 7 and 8 messages contain the extra cell selection parameters (such as CELL_RESELECT_OFFSET, TEMPORARY_OFFSET, see "Test 1 – Serving Cell Information (1)"). These parameters are broadcast on the BCCH Ext, which is an additional downlink channel obtained by taking away blocks normally used for paging(PCH)/access grant(AGCH). These parameters may also be broadcast in System Information type 4 messages, which my network, Optus, does, as Optus does not use the BCCH Ext.

Orange : The network supports Cell Broadcast SMS Messages (1=Yes, 2=No). This information is broadcast in System Information Type 4 messages. [GSM 04.12]

Grey : The network supports call-re-establishment – this is where the phone attempts to automatically re-establish the connection after a radio link failure (1=Yes, 2=No). This information is broadcast in System Information Type 1, 2, 2bis messages [GSM 04.08:4.5.1.6]

Purple : (dualband only) Early Classmark (ECSC) is supported. ECSC is where the mobile station attempts to send a classmark (it's capabilities) to the network as early as possible. This classmark may include power output, encryption, SMS, revision level (see "Test 44 – Change Revision Level value"), SS Screening indicator (see "Test 14 – Change Screening Indicator value"), and other information. This flag only displays during idle mode. In dedicated mode (call) this displays 'x'. This information is broadcast in System Information type 3 messages. [GSM 04.08:3.3.1.1.4.1,10.5.1.5,10.5.1.6,10.5.1.7]

Light Blue : (dualband only) System Information type 2Ter messages are supported. This flag only displays during idle mode. In dedicated mode (call) this displays 'x'. 2Ter messages contain information to help the MS find neighbour cells BCCH carrier channels, possibly in multiple bands. [GSM 04.08:9.1.34]

Dark Green : (dualband only) A value from 0-3 which decides how the dualband MS (phone) will report the 6 other cells to the network, value is broadcast in System Information type 2Ter message (see above). [GSM 05.08:8.4.3]

According to the GSM Specifications [GSM 05.08:8.4.3] :

- If the value is 0 the MS reports the six strongest cells whose NCC (Network Color Code) component of the BSIC (Base Station Identifying Code) is allowed (i.e. usually means part of the same network). The cells can be across any band.
- If the value is 1 the MS reports the strongest cell in each of the bands excluding the band of the serving cell. The remaining positions in the report are used to monitor the strongest cells in the band of the serving cell. If there are any leftover positions, they are filled with remaining strongest cells from any band.
- If the value is 2 the MS reports the 2 strongest cells in each of the bands excluding the band of the serving cell. The remaining positions are filled with the strongest cells of the band of the serving cell. Any leftover positions are filled with the remaining strongest cells in any band.
- If the value is 3 the MS behaves in exactly the same way as if the value was 2, however it reports the 3 strongest cells in the bands excluding the serving cell's band.

When the term 'bands' is used in the above description, it is referring to the allowed blocks of spectrum broadcast by the cell in the BCCH/SACCH, known as the BA (BCCH Allocation).

In dedicated mode, you can see the contents of the measurement report in Tests 3, 4, and 5, and how this parameter affects the contents.

In the example screen, my serving cell supports emergency calls, IMSI-attach-detach procedure, C2 values, cell broadcasts, ECSC, 2Ter messages, and reports cells using the second method described as above.

Test 08 – Multislot information

Available in: 6210

This test displays information about which timeslots are used on the current ARFCN channel. Typically, only 1 timeslot will be used (constituting one physical channel) however when using HSCSD (High Speed Circuit Switched Data) multiple timeslots can be used (meaning several simultaneous physical channels for parallel data transmission).

```
08          09:10
┌ Ts 01234537 ─┘
│ Rx xxxxxxxx │
│ Tx xxxxxxxx │
│ mCh x mPw xx │
└──────────┘
Menu      Names
08          09:13
┌ Ts 01234537 ─┘
│ Rx 00010100 │
│ Tx 00001000 │
│ mCh 5 mPw 10 │
└──────────┘
Menu      Names

08          09:13
┌ Ts 01234537 ─┘
│ Rx ██████████ │
│ Tx ██████████ │
│ mCh █ mPw █   │
└──────────┘
Menu      Names

08          09:16
┌ Ts for Rx    ─┘
│ TS for Tx   │
│ MainCh/PwrLv │
└──────────┘
Menu      Names
```

Red : Rx timeslots. Each column underneath the timeslot numbers represents that timeslot. If the value is 0, the timeslot is not used for downlink communication. If the value is 1, the timeslot is used for downlink communication (and consequently the corresponding information in Test 09 is valid). If the MS is not in dedicated mode, 'x' is displayed. [GSM 04.08:10.5.2.21b]

Green : Tx timeslots. Each column underneath the timeslot numbers represents that timeslot. If the value is 0, the timeslot is not used for uplink communication. If the value is 1, the timeslot is used for uplink communication (and consequently the corresponding information in Test 09 is valid). If the MS is not in dedicated mode, 'x' is displayed.

Blue : The timeslot number of the physical channel used to carry the DCCH (Dedicated Control Channel) signalling. From now on, 'main channel' will be used to refer to this physical channel. If the MS is not in dedicated mode, 'xx' is displayed.

Yellow : The power output used for transmission on the main physical channel. This is the same value displayed in Test 01. See Test 01 for further information. If the MS is not in dedicated mode, 'xx' is displayed.

Note the Rx and Tx configuration do not have to be the same (asymmetric). More information about multislot configurations can be found from the following reference. [GSM 05.02:B1]

Test 09 – Multislot Power Output

Available in: 6210

This test displays information about the power output on each of the physical channels used for the uplink.

```
09 10:30
┌ mCh x mPw xx ─┘
│ xx xx xx xx │
│ xx xx xx xx │
└─┘
Menu Names

09 10:31
┌ mCh 2 mPw 12 ─┘
│ xx xx 12 xx │
│ xx xx xx xx │
└─┘
Menu Names

09 10:31
┌ mCh  mPw ─┘
│  2  12 │
│  2  12 │
│  2  12 │
└─┘
Menu Names

09 10:38
┌ MainCh/PwrLv ─┘
│ PwrLv TS 0-3 │
│ PwrLv TS 4-7 │
└─┘
Menu Names
```

Red : The timeslot number of the physical channel used to carry the DCCH (Dedicated Control Channel) signalling. This is identical to the same parameter in Test 08. If the MS is not in dedicated mode, 'xx' is displayed.

Light Green : The power output used for transmission on the main physical channel. This is identical to the same parameter in Test 08. This is the same value displayed in Test 01. See Test 01 for further information. If the MS is not in dedicated mode, 'xx' is displayed.

For the following fields, the value of each field is the power output level used for the corresponding timeslot, in the same format as described in Test 01. If the MS is not in dedicated mode, or the corresponding timeslot is not used in the uplink (see Test 08), 'xx' is displayed.

Dark Blue : Timeslot 0

Yellow : Timeslot 1

Pink : Timeslot 2

Orange : Timeslot 3

Purple : Timeslot 4

Light Blue : Timeslot 5

Dark Green : Timeslot 6

Grey : Timeslot 7

Test 10 – TMSI, PRP, T3212 (Location Update) timer and AFC/AGC Information

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about the state of the location update timer, the TMSI (Temporary Mobile Subscriber Identity), the PRP (Paging Repeat Period) and the AGC/AFC (Automatic Gain Control / Automatic Frequency Control).

```
10 18:11
TMSI:11B3233B
T321: 77 80
PRP: 8 11 80
AFC 172 45
Menu Names
```

```
10 18:11
TMSI: [red] [green] [dark blue]
T321: [yellow] [pink] [orange]
PRP: [purple] [cyan]
Menu Names
```

```
10 23:44
TMSI(hex)
T321:ctr/tim
PaRP_DSF_AGC
AFC Ch
Menu Names
```

Red : TMSI – Temporary Mobile Subscriber Identity – the unique 32-bit code used by the network to identify the MS, displayed in hexadecimal. When not available (i.e. phone unable to contact network), this will be displayed as ‘x’. The TMSI is used in place of the IMSI by the network to protect user confidentiality [GSM 03.03:2.4, GSM 03.20:2.x]

Green : current value of the T3212 timer – this timer displays the length of time since the last phone location update, in units of 6 minutes (deci-hours). This timer is reset every time the phone communicates with the GSM network or when the LAC changes. [GSM 04.08:4.4.2]

Dark Blue : Maximum value of the T3212 timer. When (if) the current T3212 value reaches the max T3212 value a phone location update is performed, and the current T3212 timer is reset to 0. If this value is set to 0, the periodic location updates are not performed. Units are 6 minutes long, the maximum value is 240 (1 day). This value is assigned by the network. [GSM 04.08:4.4.2]

Yellow : PRP – Paging Repeat Period – this determines how often the phone enables its receiver to check for notifications from the network (e.g. to see if someone is calling). Units are in 51-multi-frames, which are ~253ms long. Ranges between 2-9, larger numbers mean larger periods, but less power consumption. My network, Optus, uses a fairly long value of 8 (around 2sec), Telstra uses 4 (around 1sec). [GSM 05.02:6.5.2, 6.5.3]

Pink : DSF – Downlink Signal Failure value. This value indicates the failure rate of paging messages. The counter starts at the closest integer to 90/PRP. Everytime a successful paging message is decoded, the counter is increased by 1, for every failed message, it is decreased by 4. The counter never exceeds it’s initial value. When DSF <= 0 the MS looks for a new cell. [GSM 05.08:6.5]

Orange: AGC – Automatic Gain Control value – this value shows how much the phone is adjusting its Rx sensitivity, displayed at all times, but is only correct when MS is on TCH or SDCCH. The higher the value, the weaker the signal from the BTS.

Purple : VCTCX0 AFC DAC – Automatic Frequency Control Digital to Analog Converter value – shows how much the phone is correcting its frequency to match

that of the BTS. Ranges from -1024 to +1023, the further the value is from zero, the more corrections are being made.

Light Blue : Ch – RF channel of current serving cell. If hopping is enabled, ‘H’ will appear in front of the channel number. [GSM 05.05:2.x]

Test 11 – Cell and Local Area Information

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays basic information about the current cell and local area.



Red : CC - Country Code - 3 digit country code of the current country you are in (yes Net Monitor will even tell you your country!). Australia is 505

Green : NC - Network Code - Up to 3 digit network code of the current GSM network of your country. (3 digits for GSM1900, otherwise 2 digits).

Blue: LAC - Location Area Code – 16-bit code (in decimal) of the current LA

Yellow: Ch - Channel – Up to 4 digit code of the current cell’s RF channel (ARFCN) of BCCH. If hopping is enabled, ‘H’ will appear in front of the channel number. [GSM 05.05 2.x]

Pink: CID - Cell ID – 16-bit code of cell, unique within LA. Displayed in decimal.[GSM 03.03 4.3.1]

This test is useful for distinguishing the identity of the current cell. Since channels are reused many times across the GSM network, only the LAC and the Cell ID will allow you to confirm the identify of a cell.

This test will also determine your current LAC, it is useful to see how far a LAC extends. LACs with denser coverage and mobile usage tend to be smaller. For example, the Melbourne CBD and surrounding inner-city suburbs comprise LAC 3901 on Optus. Other LACs, such as 3903 (my LAC) cover much larger areas, as these are suburbs.

When the phone cannot contact the home network, it will start monitoring other GSM networks. When the phone is in SEARch mode (See “Test 1 – Current Cell Information”), this test will display the CC, NC, LAC, Ch and CID of the monitored cell on the foreign GSM network.

As a sidenote, various network operators use conventions when defining LACs and CellIDs. For example, Singtel-Optus use the first digit of the CellID to indicate the state (3=Victoria, 2=NSW, etc), and the last digit to indicate the sector.

Test 12 – Cipher (Encryption), Hopping, DTX and IMSI status

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test shows basic information about the encryption algorithm, whether hopping is used, whether DTX (discontinuous transmission) is used as well as the IMSI-attach-detach procedure is used. This information applies to the currently registered network, or the last registered network if the phone is not currently registered to a network.

```
12 22:44
CIPHER: A51
HOPPING: ON
DTX: ON
IMSI: ON
Menu Names

12 22:44
CIPHER:
HOPPING:
DTX:
IMSI:
Menu Names

12 15:37
CipherValue
HoppingValue
DTXValue
IMSIAttach
Menu Names
```

Red – Displays the encryption algorithm used when communicating with the network. Can be “A51” (normal), “A52” (weaker), “A53” (new, very strong), or “OFF” (no encryption). This value is only displayed when the phone is communicating with the network, when idle this value is displayed as “OFF”.

Green – Displays whether frequency hopping is being used or not, displays “ON” or “OFF”.

Blue – Displays whether DTX (Discontinuous Transmission) is being used. This is where the transmitter is shut off when the user is not speaking to save power. Displays “ON” or “OFF”.

Yellow – Displays whether the IMSI-attach-detach procedure is being used. Displays “ON” or “OFF”. This is where the phone signals to the network it is available when turned on, and also signals when it is being switched off.

This test is most useful to observe what form of encryption is being used to encrypt all data between the MS and the BTS. DTX, IMSI and hopping information are repeated elsewhere.

Test 13 – DTX mode status / toggle (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test allows you to view the DTX (Discontinuous transmission) mode which controls whether the transmitter is switched off when not necessary to save power (i.e. when phone user is not speaking). It also allows the mode to be toggled on or off if the BTS allows it.

```

13 00:37
NOTALLOWED
DTX(DEF):ON
DTX(BS):USE
Menu Names

```

```

13 00:37
DTX(DEF):
DTX(BS):
Menu Names

```

```

13 15:43
DTXMode
DefaultDTXsta
DTXValFromBS
Menu Names

```

Red : Displays the status of DTX mode. Can be “DTX:ON” (in use), “DTX:OFF” (not in use), “DTX:DEF” (uses default – see next) or “NOTALLOWED” (BTS decides, not MS)

Green : MS’s default DTX mode – this is what is used if DTX Mode (above) is set to “DTX:DEF”. Can be “ON” or “OFF”.

Blue : What the BTS says to use (on BCCH(SI3) or SACCH(SI6)) – can be “USE” (must be used), “NOT” (must not be used) or “MAY” (MS can decide)

If the DTX(BS) value is set to “USE” or “NOT” (and hence the DTX mode value will be “NOTALLOWED”) the MS must do that.

If however, the DTX(BS) value is set to “MAY”, then the MS may choose and will use its DTX(DEF) value. However, jumping to this screen will allow you to specify which setting to use. Each jump will toggle between “DTX:ON”, “DTX:OFF” and “DTX:DEF”.

This is useful if you wish to flatten the phone’s battery quickly by disabling DTX and calling a number. Also, it is useful if you are interested in benchmarking talk times with and without DTX.

[GSM 04.08:10.5.2.3]

Test 14 – Change SS Screening Indicator value (active)

Available in: 5110

This test allows to select the SS Screening Indicator value that will be submitted to the GSM network in the MS Classmark 2 message.

```

14 11:48
SCREENING
INDICATOR
IS 01
Menu

```

```

14 11:48
SCREENING
INDICATOR
IS
Menu

```

```

14 15:58
Use menu to
change
screening
indicator
Menu

```

Red : The current value of the SS Screening Indicator. Viewing this test will display the value. Jumping to this test will cycle through the available values. As of GSM Phase2+, the available values are 00 and 01.

The SS (Supplementary Service) Screening Indicator is sent by the MS in the Classmark 2 Information Element at the beginning of the connection and is valid for that connection. The SS Screening Indicator informs the network about the phone's Supplementary Service capabilities, so the network knows which Supplementary Service procedures are available and what versions it can use.

The default value is 01 for a phase 2 phone, and 00 is typically used by phase 1 phones. Hence, by changing this value, you are changing the capabilities reported by the phone to the network. This is similar in principle to "Test 44 – Change Revision Level". This test has little use these days, and has been removed from newer phones.

The state of this test is not stored. When the phone is powered on, it will return to its default value (01).

[GSM 04.10:5.x, 04.80:3.7.1]

Test 15 – Multislot frames information (not functional)

Available in: 6210

This test is not functional in production models. It may have possibly being functional in development models. It seems to indicate frame transmit/receive statistics for the up to 8 physical channels.

```
15          10:43
┌──────────┴──────────┐
Tx27178506
ReTx42645758
Rx27178505
RTRq27178504
└──────────┬──────────┘
Menu      Names
```



```
15          10:41
┌──────────┴──────────┐
Sent frames
Re-transmis.
Rec. frames
Re-send reqs
└──────────┬──────────┘
Menu      Names
```

Test 17 – BTS (Base Transceiver Station) Test (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This is my favorite active test, as it allows you to lock the phone to a BTS of your choice, or more specifically, a radio channel of your choice.

```
17          11:20
┌──────────┴──────────┐
BTS_TEST
OFF
└──────────┬──────────┘
CH : 21
Menu      Names
```

```
17 11:20
BTS TEST
REQUESTED
CH : 21
Menu Names
```

```
17 11:20
BTS TEST
CH : 
Menu Names
```

```
17 15:50
Use menu to
toggle BTS
test ON/OFF
Menu Names
```

Red : Shows the status of the BTS Test. Note, this status does not always show the correct status at the time of viewing the display. Can be “OFF”, “ON” or “REQUESTED”.

Green : Shows the radio channel for BTS Testing. If no valid channel is specified in SIM location 33, “xxxx” is displayed.

BTS Test allows the user to specify a channel for testing. Once the BTS mode is engaged, only that channel is used for idle mode and active mode (although the phone is allowed to frequency hop). The phone ignores neighbour information broadcast by the tested BTS, and will not handover during call to another cell. If the phone moves out of range of the tested BTS, the phone will show no coverage and will enter NSPS (No Serve Power Save) mode until it finds another BTS using the specified channel for its BCCH. Obviously, the channel requested must be a BCCH carrier (the carrier on which information about the cell is broadcast, which phones listen to in idle mode).

To use the BTS Test mode, the radio channel to test must be entered in SIM memory location 33’s phone number. The name can be set to anything, however something like “BTS Test” would be appropriate. To find out how to store specific values to SIM memory see “ddd Storing Values to SIM Memory”. Then, jump to this test. The display will change from “BTS TEST OFF” to “BTS TEST REQUESTED”. The channel number should display the channel number you have chosen.

If the channel number displayed is “xxxx”, it means you probably have entered an invalid channel number. It also could mean the SIM card could not be read (which seems to happen sometimes after a power on). If this is the case, jump to this test to cancel the BTS Test, wait a few minutes for SIM to respond (i.e. check the phonebook for the BTS TEST entry), and then retry the test.

The state “BTS TEST REQUESTED” means the BTS Test is not actually happening, however it has been ‘scheduled’ and will occur the next time the phone loses signal. There are several ways to do this. You could attempt to disconnect the antenna or move the phone way out of coverage, often neither of these are practical or possible. Most sources recommend turning the phone off, and then back on again, which is pretty easy. There is one other way to do it however, and that is to use “Test 19 – Change Behaviour for Barred Cells” to kill the signal. See the test for more information, however to briefly describe the procedure, jump to Test 19 after requesting a BTS Test. The display should change from “CELL BARR ACCEPTED” to “CELL BARR REVERSE”. If not, keep jumping until it does display “CELL

BARR REVERSE”. Then, attempt to communicate with the network (i.e. dial a number and then a split second after pressing ‘Call’ cancel the call). Within seconds the signal should drop. To regain the signal, and enter the BTS Test, jump to Test 19 until it displays “CELL BARR ACCEPTED”. Note this procedure may not always work if there are barred cells in the area.

You can see that the BTS Test is active by viewing “Test 3 – Information about Serving Cells and Neighbours”, and you will note only the serving cell entry (the top line) is present, the neighbours are all ‘x’s. If you view Test 17 (don’t jump to it), it will also display “BTS TEST ON” and the channel number.

To disable the BTS Test, you jump to the test again, however it will still display “BTS TEST ON”. Once again, this ‘schedules’ to turn the BTS Test off the next time the phone loses coverage. One way to do this is to simply let the phone lose coverage, since it is locked to a channel, it probably will at some stage. When this does happen, the phone will search for other channels and return to normal operation. Alternatively, you can power the phone on and then off, or use the Test 19 method as described above. When the BTS Test is off again, it will display “BTS TEST OFF” and the channel number currently saved in the SIM memory.

BTS Test mode is a very powerful test, and can sometimes help in a number of situations, or is fun to play around with. See ??whatever??

A word of warning, however. BTS Test can have problems with some phones, such as earlier software on the 6210 and 8250, but there are most probably others. In some cases, I have heard, the phone might display “CONTACT SERVICE”, and can be fixed by re-flashing the software. In other cases, starting with a SIM card of a different network operator can fix the problem. Use this test at your own risk.

For some models of phones, particularly some older ones such as the 5110, this test exhibits unusual and possibly problematic behavior when paired up with Test 19 (to drop the coverage). In such a case, it is better to resort to power cycling the phone to toggle BTS Test status.

Also, on some phones, such as the 5110, the status “REQUESTED” is not displayed (it is left as “OFF”). The behavior of the test is otherwise normal.

Test 18 – Toggle backlights status (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test allows more flexible control over the LCD and keypad backlights. Typically, the backlights stay on after pressing a key (when the phone is not locked) and remain on while there is keyboard input. They will then switch off after 15 seconds of no keyboard input.

This test is an active test, meaning jumping to it will toggle its status. Viewing this test will simply show the result of the last toggle. The test toggles between “LIGHTS ON” and “LIGHTS OFF”



The behaviour might look obvious however it requires some explanation. When the test is toggled to “LIGHTS OFF” the opposite of normal behaviour will occur. That is, the lights will immediately go off, and remain off as long as a key is being pressed. If no key is pressed for 15 seconds, or you begin to type an SMS message for 10 seconds, or make a call, the phone will revert to normal behaviour as described before.

Turning the lights off is useful if you can see the display well and wish to conserve power (especially if your phone has bright modified lights!) whilst changing some settings or playing a game, but not typing an SMS, as the lights will come back on after you being typing.

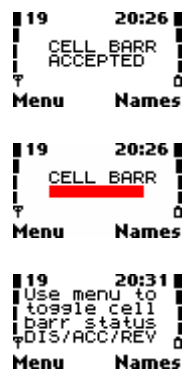
When the test is toggled to “LIGHTS ON” the lights will switch on (if not already on) and remain on as long as a Net Monitor test is displayed on the screen. Actually the lights will go out briefly after the normal time period (15 seconds) and then come back on permanently. Note if you revert to the normal home screen by jumping to test 0 the lights will revert to normal behaviour.

Keeping the lights on is useful if you wish to discharge your battery (especially if you have modified or bright lights), if you have bright lights you can also use your phone as a torch (the keypad LEDs on an 8250 are especially useful for this). Finally if you are monitoring some particular Net Monitor test (such as the field tests) in the dark you may wish to have constant illumination.

Test 19 – Change Behaviour for Barred Cells (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test allows the user to allow the phone to ignore barred cells, or use only barred cells.



Red : Displays how the phone will respond to cell barring - values are “ACCEPTED”, “REVERSE” or “DISCARD”.

Jumping to this test will cycle through “ACCEPTED”, “REVERSE” and “DISCARD”. Viewing this test will show the current behaviour in relation to barred cells.

Barred cells are those inform the MS not to camp on them in idle mode, for a reason decided by the operator, for example, the operator may be testing the cell, or would prefer the phones to camp on another cell.

When in ACCEPTED mode, which is the default, the MS behaves normally – it does not camp on these barred cells and they will have ‘B’ indicators in Tests 3-5.

When in REVERSE mode, the MS only wishes to camp on barred cells. If you select this mode, initially it will appear nothing will happen, however, after a while, the priority indicators in Tests 3-5 will change to ‘B’. This only happens after the phone reads the BCCH information from these cells (as the barring status is toggled when decoding BCCH). This can be a long time particularly when stationary (the GSM specifications allow up to 5 minutes). Barred cells will change from ‘B’ to ‘N’ (or ‘L’). However, the serving cell’s status is not updated – hence it will still serve as if it were its original priority (‘N’ or ‘L’). You can find out when BCCH carriers from neighbours are decoded in “Test 62 – Neighbour Measurement Information” and the serving cell in “Test 61 – Serving Cell Measurement Information” – the appropriate counters will increase from their previous values.

The barred status is updated for the serving cell after the phone leaves idle mode and returns to it (hence forcing cell reselection).

These characteristics have several uses. Firstly it allows a quick but not necessarily reliable locking to the current serving BTS, provided there are no barred cells in the area. By changing the status to “REVERSE” the other cells will eventually be marked barred, hence the MS has no choice but to stay on the serving cell. Changing the status to “DISCARD” or “ACCEPTED” will undo this behaviour.

Secondly, this can be a quick way to kill the phone’s coverage and make it enter the search state. By setting the status to “DISCARD”, and making a communication with the network (such as request a call divert status or start to make a call and quickly terminate it), when the phone returns to idle mode, it will see all cells as ‘barred’ and only select one that is really barred. If no such cell exists, the phone will lose coverage. This is particularly useful when partnered with “Test 17 – BTS Test”. When the phone does lose coverage, it may also show interesting information. On newer phones it seems, it will occasionally jump to BCCH carriers (of all networks) and show parameters from those networks, in the various tests. On some other phones, such as the 5110, it will fully monitor the network (all displays, including all of Tests 3-5 – not just serving cell, as well as continually updating this information), before possibly hopping to another network if there are no cells it can camp on (no barred cells).

Note that barred status applies only to idle mode – it does not prohibit the phone from handing over to the cell during a connection.

The final status, “DISCARD” means cell barring information broadcast in the cell’s BCCH is ignored. In other words, barred cells are treated as normal cells, and normal cells are treated normally. This technically can be used to ‘expand’ your coverage however in reality it will probably do very little. Many network operators (including Optus) do not use the cell bar feature.

The status of this test is not preserved across a reboot; the phone will power on with the default setting of “ACCEPTED”

[GSM 03.22:3.x,4.x 05.08:6.1,6.2,6.3,6.4,6.6]

11. Battery/Power Tests – Tests 20 – 23

Test 20 – Battery and Charging Information

Available in 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays general information about the phone’s battery and charging information (if it is being charged)

```
20      16:32
382  XXXXX
T+25  W  0
C      696  6976
Menu  Names
```

```
20      16:35
396  LithC
T+26  W255 1
C      709  6976
Menu  Names
```

```
20      16:32
T      █
C      █
W      █
Menu  Names
```

```
20      16:39
BatVol ChMod
BTemp ChTime
ChrVol Pwm
BTYP  BFDC
Menu  Names
```

Red : The current voltage across the battery’s terminals, in hundredths of a volt (e.g. 382 means 3.82V). You will notice that this value will generally decrease the more the battery is loaded (i.e. when backlight turns on, when transmitter is active). Also, generally as the battery drains, the battery voltage will decrease as well, especially when the battery is approaching it’s ‘flat’ point; this value will more quickly. For example, an 8210 (with 750mAh BLB-2) went down to 3.09V in standby, at this point the phone would immediately shut off if I attempted to use the transmitter (i.e. make a call), shortly after the phone shut off with the message “Battery Empty”. On the other hand, a freshly charged 750mAh BLB-2 battery displayed 4.2V in standby.

Green : The state of the charging process – a 5 character word which can be:

- xxxxx – The battery is not being charged (no charger connected or there is no battery)
- InitC - The charging process is starting up. This appears briefly after the charger is connected.
- FastC - The Ni-MH battery is being fast charged, this is where a large charging current is delivered
- TxOnC – The Ni-MH battery is being charged, and the transmitter is on. ?????
- FullM – The Ni-MH battery has been fully charged. It is now being maintenance (trickle) charged to keep topped up.
- LithC – The Li-Ion battery is being charged.
- LiTxO – The Li-Ion battery is being charged, and the transmitter is on.
- LiAFu - The Li-Ion battery's charge current has been temporarily suspended, as the PWM (see below) duty-cycle value has fallen too low to keep it charging. When this occurs the PWM value is usually increased slightly, as well as the charge counter (see below).
- LiFul - The Li-Ion battery's PWM duty-cycle value has fallen too low for a period of time long enough that the charge counter has expired. This means the battery is finished charging, and "Battery Full" is displayed.
- LNFTx – The Li-Ion battery was full, not being charged, and the transmitter is on. The battery seems to supply the current to operate the transmitter, as charging seems to recommence afterwards.

Dark Blue : The internal temperature of the battery, in degrees Celsius. The temperature is measured to assist in the charging process, such as possibly monitoring if the charge current is too high (battery is too hot) and possibly in the battery full detection (so the phone knows when to back off on the charging). For those who had the idea of using this as a simple thermometer, it won't work.

Yellow : The period of time the phone has been charging, format is hmm - first digit is hours, next two digits are minutes. This counter is reset whenever the charger is connected and charging begins. It is also reset in some models at the end of use of a TCH (e.g. call) during charging. There are occasionally some exceptions, such as when the charger is reconnected after it was disconnected during certain phases of charging. This counter increases when the phone is off too, however under some circumstances may be reset when the phone is powered on.

Pink : Charge voltage, in deci-volts (tenths of a volt - e.g. 44 is 4.4V) The voltage being used to charge. In Ni-MH charging, this fluctuates greatly but in Li-Ion charging this rises during the initial charge phase, and stays fairly constant during the remaining charging (as is required for Li-Ion charging), with the occasional spike. Note this seems to be higher (such as 4.3V) than 4.2V which is the maximum charging voltage for most Li-Ions. Presumably this is therefore not the direct voltage that is driven to the battery terminals, but further back in the circuitry. Charging voltage appears as 0V obviously when not charging.

Orange : The Pulse Width Modulation (PWM) duty-cycle. In Li-Ion charging, near the end of the charge, the charging current is no longer constantly applied to the battery – it is pulsed, initially with long pulses, then becoming shorter and shorter until the battery is fully charged. The duty-cycle can be calculated by PWM/255, hence a value of 0 means no charge voltage is being applied (e.g. charger not connected, or in a temporary suspended state such as LiAFu), and 255 means a continuous voltage (during early-mid Li-Ion charging and for all Ni-MH charging). Hence a value of 128 means half the time the pulses are applied, and the other half

they are not. In some phones, with bright LEDs, the charge pulses can be faintly observed in the LEDs having slight brightness fluctuations. The frequency of the PWM process is about 1Hz, so a PWM value of 128 means the pulses are applied for about 500ms, and relaxed for about 500ms. Ni-MH batteries are not pulse-charged at any point and hence this value is 255 (constant voltage DC).

Light Blue :

Comment here...

Test 23 – Information about Battery and Battery Use

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays more general information about the battery, and also current consumption and voltage levels.



Dark Blue : The charging current being delivered to the battery, in milliamps. This value generally stays constant during both Ni-MH charging and Li-Ion charging (except when using ACP-7A), except when in the end stage of Li-Ion charging, during which the current is pulsed (See “Test 20 – Battery and Charging Information”). During the pulsed charging, the value will usually fluctuate between 0 and the actual charging current, depending on whether the latest sample was taken during a pulse or not. The maximum value of this charging current varies depending on the charger’s capacity – around 350mA on the ACP7A, 600-700mAh on the ACP8A, and 800-850mA on the ACP12A.

Light Blue : The current power consumption of the unit, in milliamps. This is an interesting value, you will notice it changes depending on what the phone is doing. If the lights come on, you will notice the power consumption increases greatly. If the transmitter is going (see “Test 1 – Serving Cell Information (1)”) the power consumption will increase even more (varies depending on how hard the transmitter is outputting and which band). This value is not actually measured it seems, but calculated based on pre-known values by the phone. This is why, for example, if the backlight LEDs have been changed, and usually consume more power especially if the resistors have been bypassed, it is not reflected here.

12. Misc. Phone Software and Status Information – Tests 30 - 39

Test 35 – Reason for Last Software Reset

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about why the phone's software (firmware) was last reset.



Red : The reason for the last software restart. Can be “NORM”, “UNKNO”, “HW WD”, “SWDSP”, “STACK”, “SWIDL”, or “SWSIM”.

The reasons are as follows:

NORM – A normal phone software start, this includes restarts from software like LogoManager.

UNKNO – The reason for the software restart was unknown

HW WD – This is the hardware watchdog – which monitors signals from the phone's software. If the software freezes, these signals are not generated and the hardware reboots the phone.

SWDSP – DSP recovery reset

STACK – one of the task stacks overflowed. The offending task should be listed in the next field, and more about the process's current stack in “Tests 84-87 Information about task stacks and message buffers”. You can also identify the stack in “Test 57 – Memory and Stack status before Reset”.

SWIDL – The idle task stopped running

SWSIM – Error with SIM card – could be communication problem, or as a result of attempting to unlock

Green : The running task at the time of the restart, or “UNKNOWN” if not known. You can find out about your phone's task by looking at the help screens of “Tests 84-87 – Information about task stacks and message buffers”

Note this information is stored in EEPROM, and hence is only updated with a proper reset. By truly powering off the phone (e.g. by disconnecting battery) the values will not be updated and the last reason for software reset (prior to powering off) will still be shown after power on. “Test 36 – Software Reset Statistics” keeps a tally of the various reset reasons

Test 36 – Software Reset Statistics

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test shows the history of the reset reasons described in “Test 35 – Reason for Last Software Reset”.



Red : Number of unknown resets (described as “UNKNO” in Test 35)

Green : Number of resets due to hardware watchdog (described as “HW WD” in Test 35)

Blue : Number of resets due to DSP recovery reset (described as “SWDSP” in Test 35)

Yellow : Number of resets due to SIM related errors (described as “SWSIM” in Test 35)

Pink : Number of resets due idle task not running (described as “SWIDL” in Test 35)

Orange : Number of resets due to stack overflow. (described as “STACK” in Test 35)

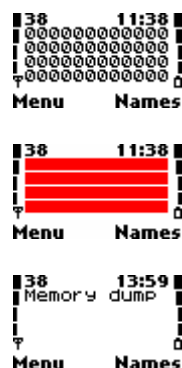
These counters are saved in the EEPROM and are not reset on reboot. There is no test to reset them, not even “Test 240 – Reset all”. The only way is with service software or by modifying the EEPROM contents.

It can be seen in the two-year life of this particular phone (EEPROM never cleared), there have been relatively few resets due to errors. The exception is the hardware watchdog resets (18 occurrences), which seemed to occur with one particular SIM I used for several months (A Virgin Mobile SIM), where the phone would freeze.

Test 38 – Memory Dump (active)

Available in: Nokia debugging firmware, unknown models.

This test allows a selected portion of memory to be viewed.



Red : 48 hexadecimal digits corresponding to a contiguous 24 byte memory dump starting at the specified memory address. Memory is read the way you would read a book (left-right, top-bottom).

The starting address is specified by entering the required 24-bit address in hexadecimal into the name (alpha) field of SIM location 30. To find out how to store specific values to SIM memory see “ddd Storing Values to SIM Memory”.

Once the address is entered, jumping to this test will update the display with the new memory region.

Unfortunately this very interesting test appears very rarely, in debugging firmware.

Test 39 – Reason for Last Call Release

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays the reason the last call terminated and at what sub-layer of the layer 3 protocol it occurred.



Red : The reason for the last call release in the Call Control sub-layer.

Green : The reason for the last call release at the Mobility Management sub-layer.

Blue : The reason for the last call release at the Radio Resource sub-layer.

This test allows the user to see in more detail the reason a particular call ended, and at which sub-layer of the layer 3 protocol it occurred in. The layers of the GSM system on the MS-BTS interface are described in GSM 04.04 (layer 1), GSM 04.05, GSM 04.06 (layer 2), GSM 04.07, GSM 04.08 (layer 3).

The individual cause values are described in Annex F (RR), Annex G (MM) and Annex H (CC) of GSM 04.08, however, the more common ones are summarized below:

Radio Resource:

0 – Normal release of RR connection.

1 – Abnormal release, reason not specified

2- Channel unacceptable

3 – Timer expiry (one of the timers expired and the connection was released)

- 4 – No activity on radio path (the BTS does not detect transmission when there is supposed to be)
- 5 – Preemptive release – the network released the RR connection due to
- *8 – Handover impossible; timing advance out of range
- *9 – Channel mode unacceptable (MS cannot support the channel configuration assigned by the network)
- 65 – Call already cleared – the handover failed as the connection had already been released

Causes 95-111 are associated with protocol error

- 95 – Semantically incorrect message
- 96 – Invalid mandatory information
- 97 – Message type non-existent or not implemented
- 98 – Message type not compatible with protocol state
- 100 – Conditional IE error
- 101 – No cell allocation available
- 111 – Protocol error unspecified

* These causes are sent to the network, otherwise the cause is sent by the network (in CHANNEL RELEASE message)

Mobility Management:

- 2 – IMSI unknown in HLR – The IMSI is not known by the network
- 3 – Illegal MS – the MS is refused service as the authentication failed
- 4 – IMSI unknown in VLR
- 5 – IMEI not accepted – network does not allow emergency calls using IMEI as identification (all Australian networks do)
- 6 – Illegal ME – sent when the network does not accept the IMEI, i.e. due to stolen phone blacklisting
- 11 – PLMN not allowed – used when the MS attempts location updating and the network forbids it to
- 12 – Location area not allowed – used when the MS attempts location updating in an area the network forbids it to
- 13 – Roaming not allowed in this area – used when the MS attempts location updating in an area it is roaming and the network forbids it to.
- 17 – Network failure – the network sends this if a fault has developed in the network
- 22 – Congestion – the network sends this if the network has become too congested to proceed
- 32 – Service option not supported – the network sends this in a CM SERVICE REJECT message when the MS requests an unsupported service in the CM SERVICE REQUEST message.
- 33 – Service option not allowed due to subscription – the network sends this in a CM SERVICE REJECT message when the MS requests a service it does not have a subscription to (i.e. not enabled on the subscribers account)
- 34 – Service option temporarily not available – the network sends this in a CM SERVICE REJECT message when the MS requests a service that is temporarily unavailable due to technical failure

38 – Call cannot be identified – This cause is sent when the MS attempts to re-establish an MM connection after a radio-link failure, however the network was unable to associate the request with the failed connection

Causes 95-111 are associated with protocol error

95 – Semantically incorrect message

96 – Invalid mandatory information

97 – Message type non-existent or not implemented

98 – Message type not compatible with protocol state

99 – Information element non-existent or not implemented

100 – Conditional IE error

101 – Message not compatible with protocol state

111 – Protocol error unspecified

Call Control

Normal causes:

16 – Normal call clearing – the call was cleared because one of the users requested it to be cleared

17 – User busy – the called user indicated he was unable to take the call (i.e. rejected the call)

18 – No user responding – the called user's equipment did not respond

19 – No answer – the called user's equipment responded, but the user failed to answer it

21 – Call rejected – the call was rejected as the equipment was not technically able to receive the call

22 – Number changed – the called number no longer exists. The new number may optionally be returned with this cause

25 – Preemption – the network released the call in order to free resources for a call of higher priority

27 – Destination out of order – The called party cannot be reached because of a technical failure at the destination user's end of the connection

28 – Invalid number format – the phone number was not a valid format

31 – Unspecified normal clearing (used when causes 1-28 do not apply)

Resource unavailable causes:

34 – No circuit/channel available – phone displays 'Network Busy'

38 – Network out of order – A failure in the network stopped the call, and it is likely to last for a while, such as that re-attempting the call is not likely to work

41 – Temporary failure – a failure in the network stopped the call, but it is likely to last only a short time, suggesting to re-attempt the call

42 – Switching equipment congestion – congestion in the switching equipment stopped the call

44 – Requested circuit/channel not available – no resources available to the remote user

47 – Resource unavailable due to unspecified reason (used when causes 34-44 do not apply)

Service/option unavailable causes:

- 49 – Quality of service not available
- 55 – Incoming calls barred within Closed User Group – incoming calls are not allowed in this CUG
- 57 – Bearer capability not authorized – the MS requested a bearer capability it is not authorized to use
- 58 – Bearer capability not presently available – the MS requested a bearer capability that is not available at the time of request
- 63 – Service or option not available due to unspecified reason (used when causes 49-58 do not apply). I have noticed this when trying to make a call on Line 2, trying to make a data call on an account without data service, etc.

Service/option not implemented causes:

- 65 – Bearer service not implemented – the equipment sending the cause does not support the bearer capability requested
- 69 – Requested facility not implemented – the equipment sending the cause does not support the supplementary service requested
- 70 – Only restricted digital information bearer capability is available – the equipment sending this cause only supports a restricted version of the requested (unrestricted) bearer capability
- 79 – Service or option not implemented due to unspecified reason (used when causes 65-70 do not apply)

Invalid message causes:

- 81 – Invalid Transaction Identifier (TI) – invalid transaction identifier received (a value in the layer 3 header which uniquely identifies a connection amongst the stream of data)
- 87 – User not member of CUG (Closed User Group) – The called user for the CUG call is not a member of that CUG
- 88 – Incompatible destination – the sender of this cause cannot meet the establishment requirements requested
- 95 – Semantically incorrect message – the sender of this cause has received a message with semantically incorrect contents

Causes 96-111 are associated with protocol error

- 96 – Invalid mandatory information
- 97 – Message type non-existent or not implemented
- 98 – Message type not compatible with protocol state
- 99 – Information element non-existent or not implemented
- 100 – Conditional IE error
- 101 – Message not compatible with protocol state
- 102 – Recovery on timer expiry
- 111 – Protocol error unspecified

13. Layer 1/Layer 2 statistics and Various Controls – Tests 40 - 45

Test 40 – Reset Handover Counters (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test resets the handover counters in “Test 41 – Inter-cell Handover Counters”, “Test 42 – Intra-cell Handover Counters” (if present) and “Test 43 - Layer 2 (Data Link) Timeout Counters”

```
40 00:17
  RESET
  HANDOVER
  COUNTERS
  Menu Names

40 16:02
  Use menu
  to reset
  handover
  counters
  Menu Names
```

By jumping to this test the handover counters will be reset. The display will not change.

Test 41 – Handover Counters (singleband phone)

Available in: 5110

This test displays the handover statistics. See more about handovers in “x.y Handovers”

```
41 13:19
  HandOOk : 903
  PrevCh  : 51
  HONoOk  : 7
  HOIntra : 771
  Menu

41 13:19
  HandOOk :
  PrevCh  :
  HONoOk  :
  HOIntra :
  Menu

41 18:33
  HandOvOkCntr
  PrevChanCntr
  HandOvNoOkCntr
  HOIntraOkCntr
  Menu
```

Red : Number of successful handovers. (?? Does include intras ??)

Green : Number of successful returns to previous channel.

Blue : Number of failed handovers.

Yellow : Number of successful intra-cell handovers.

The maximum value of these counters is 9999. When a counter reaches 9999, (?? All ??) counter will stop.

It can be seen that the single-band handover counters screen is less detailed than the dualband ones, i.e. there are no separate failed/back to previous statistics for Intra-cell and Inter-cell handovers.

These counters can be reset to 0 with “Test 40 – Reset Handover Counters” or “Test 60 – Reset Field Test Counters”.

Test 41 – Inter-cell Handover Counters (dualband phone)

Available in: 2100, 3330, 6150, 6210, 7110, 8210, 8250

This test displays the handover statistics for inter-cell handovers, that is, handover during dedicated mode (call) between two different cells. The cells may be controlled by the same BSC, controlled by separate BSCs with the same MSC, or controlled by separate BSCs each attached to different MSCs (possibly even handover to a different network). See more about handovers in “x.y Handovers”.



- Red** : Number of successful inter-cell handovers within the GSM900 band
- Light Green** : Number of successful inter-cell handovers from within the GSM1800 band
- Blue** : Number of successful inter-cell handovers from the GSM900 band (old cell) to the GSM1800 band (new cell)
- Yellow** : Number of successful inter-cell handovers from the GSM1800 band (old cell) to the GSM900 band (new cell)

Maximum value of successful counters is 9999.

- Pink** : Number of failed inter-cell handovers from within the GSM900 band
- Orange**: Number of failed inter-cell handovers from within the GSM1800 band
- Purple** : Number of failed inter-cell handovers from the GSM900 band (old cell) to the GSM1800 band (intended new cell)
- Light Blue** : Number of failed inter-cell handovers from the GSM1800 band (old cell) to the GSM900 band (intended new cell)

Maximum value of failed counters is 999

- Dark Green** : Number of successful inter-cell returns to previous channel from within the GSM900 band.
- Grey** : Number of successful inter-cell returns to previous channel from within the GSM1800 band.

Red-Blue : Number of successful inter-cell returns to previous channel from the GSM900 band (old cell) to the GSM1800 band (new (original) cell)

Green-Yellow : Number of successful inter-cell returns to previous channel from the GSM1800 band (old cell) to the GSM900 band (new (original) cell)

The 'return to previous' handover is where the MS fails to connect on the new channel and re-establishes communication on the previous channel, hence maintaining the connection. Maximum value of return to previous channel counters is 999.

When one of the counters reaches the maximum value, the counters (all?) will stop.

These counters can give an indication of how much the phone is changing cell, often as a result of moving through the GSM network. It can also give an indication as to what bands the phone is using the most. In my example, I live in a suburban area with heavy GSM usage and hence there is both GSM900 and GSM1800 coverage. It can be seen that my phone often uses GSM1800 due to the high GSM900→GSM1800 and GSM1800→GSM900 handover values (relative to the GSM900→GSM900 handover values).

These counters can be reset to 0 with "Test 40 – Reset Handover Counters" or "Test 60 – Reset Field Test Counters".

Test 42 – Intra-cell Handover Counters (dualband phone)

Available in: 2100, 3330, 6150, 6210, 7110, 8210, 8250

This test displays the handover statistics for intra-cell handovers, that is, handover during dedicated mode (call) between different channels within the current cell. See more about handovers in "x.y handovers". This test only appears in dual-band phones.

```
42 17:58
392 24
0 0 0 0
1 0 0 0
Menu Names
```

```
42 17:58
[Red] [Light Green]
[Blue] [Yellow]
[Green] [Orange]
[Light Blue] [Purple]
Menu Names
```

```
42 16:41
G>G IntraD>D
G>D OK D>G
IntraHoFail
Back ToPrev
Menu Names
```

Red : Number of successful intra-cell handovers within the GSM900 band

Light Green : Number of successful intra-cell handovers from within the GSM1800 band

Blue : Number of successful intra-cell handovers from the GSM900 band (old channel) to the GSM1800 band (new channel)

Yellow : Number of successful intra-cell handovers from the GSM1800 band (old channel) to the GSM900 band (new channel)

Maximum value of successful counters is 9999.

Pink : Number of failed intra-cell handovers from within the GSM900 band
Orange: Number of failed intra-cell handovers from within the GSM1800 band
Purple : Number of failed intra-cell handovers from the GSM900 band (old channel) to the GSM1800 band (intended new channel)
Light Blue : Number of failed intra-cell handovers from the GSM1800 band (old channel) to the GSM900 band (intended new channel)

Maximum value of failed counters is 999

Dark Green : Number of successful intra-cell returns to previous channel from within the GSM900 band.

Grey : Number of successful intra-cell returns to previous channel from within the GSM1800 band.

Red-Blue : Number of successful intra-cell returns to previous channel from the GSM900 band (old channel) to the GSM1800 band (new (original) channel)

Green-Yellow : Number of successful intra-cell returns to previous channel from the GSM1800 band (old channel) to the GSM900 band (new (original) channel)

The ‘return to previous’ handover is where the MS fails to connect on the new channel and re-establishes communication on the previous channel, hence maintaining the connection. Maximum value of return to previous channel counters is 999.

When one of the counters reaches the maximum value, the counters (all?) will stop.

It can be seen on my example, that intra-cell handovers do not occur frequently. Also, the cross band (GSM900 → GSM1800 and GSM900 → GSM1800) are zero as my network, Optus, does not mix bands on the same cell, a separate cell is used for each (even though they are on the same physical structure and probably have same BSC). I am not too sure about other networks, I believe Telstra does this differently, I will investigate this further.

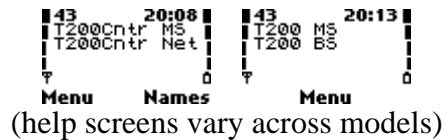
These counters can be reset to 0 with “Test 40 – Reset Handover Counters” or “Test 60 – Reset Field Test Counters”.

Test 43 – Layer 2 (Data Link) Timeout Counters

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This information shows the state of the T200 counters.





Red : Number of T200 expirations for the MS (phone).
Green : Number of T200 expirations for the BS (network).

The T200 timer is used by the data link layer to timeout unacknowledged frames (for frames transmitted in acknowledged mode). When some form of acknowledgement from the remote entity is received, this timer is reset. If this timer expires, re-transmission occurs. This is somewhat like the Internet's TCP behaviour.

[GSM 04.06:5.x]

These counters are saved in EEPROM, and are not cleared when reset. These counters will stop when they reach their maximum value (9999).

These counters can be reset to 0 with "Test 40 – Reset Handover Counters" or "Test 60 – Reset Field Test Counters".

Test 44 – Change Revision Level (active)

Available in: 5110

This test allows the user to change the revision level.



Red : The current value of the revision level. As of Phase2+, valid values are 00 (Phase 1) and 01 (Phase 2 and onwards).

The revision level is submitted to the network in the Classmark 1 and Classmark 2 Information Elements at the start of an MM connection or when requested by the network. The revision level allows the network to distinguish between Phase 1 and Phase2 and onwards mobile stations, and hence apply the appropriate protocols and procedures with them. As with "Test 14 – Change SS Screening Indicator", this test has little use these days, and has been removed from newer phones. Perhaps it could be used in a buggy older Phase2 network which has problems? [GSM 04.08]

Test 45 – Toggle Transmitter On/Off (active)

Available in: 2100, 3330*, 5110, 6150?, 6210*, 7110*, 8210*, 8250*

This test allows the user to toggle whether the transmitter can be used.



Red : Displays the state of the transmitter “ENABLED” or “DISABLED”. Jumping to this screen toggles the state.

This test allows the simulation of a scenario in which the MS can hear the BTS, however the BTS cannot hear the MS. This can happen as the BTS has a much more powerful transmitter than the MS. When the transmitter is in the “DISABLED” state, the rest of the phone’s software will assume that the signals are being transmitted – the other tests will reflect this such as Test 1, and the phone will act exactly as if the above scenario was occurring. Note on some (all?) models emergency calls will also fail.

This test is also useful if you wish to monitor the network uninterrupted by phone calls, or you wish to disable location updating as you move through the network.

*Note, on some models, particularly the more recent ones, this test does not work at all. The screen will toggle between “ENABLED” and “DISABLED” when jumped to, however nothing else will happen and the phone will behave as normal.

14. Memory and SIM Information – Test 51 – 57

Test 51 – Information about SIM

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about the SIM and the phone’s communication with it.



```

51          20:33
Vsel Bau SA1
SCond CStop
PIN1Z PUK1Z
ATR FE/PE
Menu      Names

```

Red : Voltage of Vcc (SIM voltage), in volts. Can be 3V, 5V or 3/5V (??).

Light Green : Speed enhancement parameters. Expressed as the value of F/D (for example 372 is the default F=372, D=1, and 64 is F=512, D=8). The Elementary Time Unit (etu) can hence be calculated as $etu = (F/D)(1/fs)$ seconds, where fs is the clock frequency. Hence, smaller F/D means faster communication. [ISO7816-3, GSM 11.11:5.8.3]

Dark Blue : Indicates whether the SIM card allows the clock to be stopped to save power. Either “YES” or “NO”. This information can also be found with the code *#746025625# (“*#sim clock#”).

Yellow :

Pink : The number of remaining attempts left to enter the PIN code. This code is often entered when starting the phone, or when changing settings that require authorization. When this code is incorrectly entered, the counter is decremented. When the counter reaches 0, the phone will ask for the PUK code. The initial value varies depending on the SIM, but usually is 3 attempts (GSM specification 11.11 seems to always refer to 3). When the PIN is correctly entered, the counter is reset to its initial value (after a very short period). [GSM 11.11:8.9]

Orange : The number of remaining attempts left to enter the PIN2 code. This counter behaves as described above.

Purple : The number of remaining attempts left to enter the PUK code. This code is required when the PIN code attempts have been expired, and the PUK code is required to unblock and enter a new PIN. When this code is incorrectly entered, the counter is decremented. When the counter reaches 0, the PIN can never be used and hence most features of the SIM are useless. The initial value is usually 10 (GSM specification 11.11 seems to always refer to 10). When the PUK code is correctly entered, this counter is returned to its initial value, the new PIN is assigned, and the PIN attempts counter is also returned to its initial value. [GSM 11.11:8.13]

Light Blue : The number of remaining attempts left to enter the PUK2 code, which unblocks the PIN2 code if the PIN2 code attempts have been expired. The counter behaves as described above.

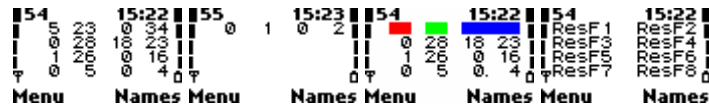
Dark Green : ATR reset counter. The number of times the ATR has needed to be retransmitted. The Answer-To-Reset is a sequence sent by the card on the I/O pin when the phone applies the correct sequence to the RESET pin. The ATR sequence describes the parameters and capabilities of the SIM, such as communication speed, clock stop capabilities etc and details about the protocol. If the ATR is not received successfully, or it includes parameters that are incompatible or invalid, the phone must attempt to reset it at least 3 times before giving up. Normally this counter is 0 (i.e. the ATR was sent once and was successful). [ISO7816-3, GSM 11.11:5.10]

Grey : Frame error or parity error counter. This displays either the number of frame errors (information in a data frame is invalid) or parity error (i.e. a byte was transmitted incorrectly). The first two characters indicate the type of error ‘FE’ and ‘PE’ for frame and parity errors respectively. The next two characters form a hexadecimal counter of the number of that type of error.

Test 54, 55 – Information about Memory Block Sets

Available in: 5110, 6150, 6210, 7110, 8210, 8250

These tests display information about the current and peak usage of memory block sets.



The format is as follows: Each screen is divided into a maximum of 8 entries, in 2 columns of 4 rows. Each entry is formatted as shown by the **Red** and **Green** fields.

Red : The number of allocated/reserved blocks in this block set (group of blocks).

Green : The fewest number of blocks that have been free in this block group. This shows the peak usage of the blocks. This value can only decrease, when a new maximum number of blocks are used.

Each entry represents a block set of memory. The top left entry of Test 54 represents Block Set 1, the top right represents Block Set 2 and so on. The number of block sets varies depending on how much memory the phone has. For example, the 8210 has 10, 7110 has 11. Some phones may not even have Test 55 as they have no more than 8 block sets.

The help screens can be used to indicate the block set as well, each entry will be replaced by text of the form “ResFx” where x is the block set number. These block sets correspond to those in “Test 57 – Stack and Memory status before Reset”.

Test 56 – Information about Double Memory De-allocations

Available in: 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about double memory de-allocations, where a task attempts to free memory that is already free.



Red : The 24-bit hexadecimal memory address of the code that called the double de-allocation. This will be displayed as ‘x’s if unknown (i.e. no double de-allocations in phone history).

Green : A counter of double de-allocations in phone history. Obviously, if this value is 0, the other values are invalid (since there have been no double-deallocations).
Blue : The name of the task which called the double de-allocation. Once again, this is meaningless if there have been no double-deallocations. It will seem to show a number of different tasks if this is the case.

These values are not cleared on reset.

Test 57 – Stack and Memory status before Reset

Available in: 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about the state of the stacks (whether an overflow occurred) and the state of the memory blocks (which were full) at the time of the last reset.



Red : Shows the state of the stacks before the last reset. Each digit corresponds to one of the task stacks, explained in more detail in “Test 83 – Change Information Shown in Tests 84-87 (active)”. The digits read left to right, top to bottom (logically). 1st digit corresponds to the top left task on Test 84, 2nd digit corresponds to top right task on Test 84, and so on. A value of 1 indicates the stack overflowed and caused the reset (see “Test 35 – Reason for Last Software Reset”). A value of 0 indicates the stack was fine and did not overflow. You may wish to then use Tests 84-87 to keep an eye on the stack usage of the offending task, and see under which circumstances it grows too large.

Green : Shows the status of each block set before reset. Each digit corresponds to one of the block sets, which are groups of memory blocks and correspond to the values of Tests 54-55. Read from the left to right. A value of 0 indicates the block set was OK before reset (not full), a value of 1 indicates the block set was fully allocated before reset (this is still OK). A value of 2 indicates a double de-allocation occurred in this block (where memory is de-allocated more than once) or the block became corrupted in some way.

These tests are only valid if the phone reset due to stack (STACK) or unknown (UNKNO) reason. See “Test 35 – Reason for Last Software Reset”. The number of values will vary from phone to phone (depends on number of tasks for stacks, and amount of memory for block sets). On some phones information may be displayed at other times, but in some other phones (such as 3310), ‘x’'s are displayed.

15. Network Related Statistics – Test 60 – 66

Test 60 – Reset Field Test Counters (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test resets to 0 the counters in “Test 65 – SMS Counters”, ..., and also the handover counters (“Test 41 – Handover Counters (singleband)”, “Test 41 – Inter-cell Handover Counters (dualband)” and “Test 42 – Intra-cell Handover Counters (dualband)” if present).

```
60 20:16
FIELD TEST
DISPLAY
COUNTERS
RESET
Menu Names
```

```
60 13:22
Use menu to
reset field
test display
counters
Menu Names
```

By jumping to this test all of the mentioned counters will be reset. The display will not change.

Test 61 – Serving Cell Measurement Information

Available in 5110, 6150, 6210, 8210, 8250

This test displays counters regarding measurements of the serving cell.

```
61 13:47
NOPSW :0507
SYNCR :2879
RESELEC:13CC
RM MonTO:0001
Menu Names
```

```
61 13:47
NOPSW :
SYNCR :
RESELEC:
RM MonTO:
Menu Names
```

```
61 00:11
PSWMeasCntr
SynCMeasCntr
CellReseICtr
RM Mon TOuts
Menu Names
```

Note the bottom line only displays on certain (generally newer phones)

Red :

Green : The number of times (in decimal) the MS has attempted to synchronize to the serving cell. Synchronization is where the MS listens to the SCH channel on timeslot 0 of the radio channel containing the BCCH. When it receives a synchronization burst, it uses it to set up its internal timings and frame numbers, so it can determine which timeslot is which, which frame is which, etc. This value usually only increases on power on (to synchronize to a BCCH carrier), or when the phone loses coverage. [GSM 05.08:6.x, 05.10:4.x]

Blue : The number of times (in hex) the MS has reselected a new cell for camping on in idle mode. Cell reselection occurs when a suitable neighbour cell has a higher C2 value for a period (usually 5 seconds), often at the end of a call, or after a DSF. See “Test 1 – Serving Cell Information (1)”, “Test 2 – Serving Cell Information (2)” and

“Test 10 - TMSI, PRP, T3212 (Location Update) timer and AFC/AGC Information”. You will notice if you are moving through an urban area this counter will increase very rapidly (due to the small size and large number of cells). [GSM 05.08:6.x]

Yellow :

These counters can only be reset with “Test 60 – Reset Counters”. The values are stored in the EEPROM, and are preserved across reboots, SIM card changes, and even software upgrades (provided the EEPROM is not cleared). Note, they are only saved when the phone is properly powered off, hence if the phone crashes or the battery is removed, the totals will not be updated.

Test 61 – Serving Cell Measurement Information (2100, 33xx)

Available in: 2100, 3310, 3330, 7110

This test displays counters regarding measurements of the serving cell.



Red :

Green : The number of times (in decimal) the MS has attempted to synchronize to the serving cell, as described in “Test 61 – Serving Cell Measurement Information”

Blue : The number of times (in decimal) the MS has reselected a new cell for camping in idle mode, as described in “Test 61 – Serving Cell Measurement Information”

Yellow :

This test is identical to “Test 61 – Serving Cell Measurement Information”, however, the screen is just formatted differently.

Test 62 – Neighbour Measurement Information

Available in: 5110, 6150, 6210, 8210, 8250

This test displays counters regarding measurements of neighbour cells.



```

62      00:25
NeahrPswCtr
SyncMeasCntr
BCCHMeasAtmp
BCCHExtMeAtm
Menu    Names

```

Red : ...

Green : The number of times (in hex) the MS has attempted to synchronize to neighbour cells for the purpose of taking measurements and decoding their BCCHs. This value increases continually. This value is represented [GSM 05.08:6.x,8.x 05.10:4.x]

Blue : The number of times (in hex) the MS has attempted to decode the BCCH (Broadcast control) information of the neighbour cells. The BCCH information is decoded in order to obtain the parameters needed for the cell reselection algorithm. The GSM specifications state this information shall be decoded at least every 5 minutes, and within 30 seconds when a BTS enters the ‘strongest 6’ list. This parameter will update much more frequently if an MS is moving through the GSM network, as more and more new cells (identified by BCCH carrier and BSIC) are discovered. The BCCH information is not decoded whilst in a call as only the signal strength of the BCCH is measured and submitted in the measurement report. The network already knows the BCCH information when ordering a handover. [GSM 05.08:6.6.1]

Yellow : The number of times (in hex) the MS has attempted to decode the BCCH Ext (Broadcast control extension) of the neighbour cells. The BCCH Ext is used to broadcast additional messages (supplements BCCH), and is formed by taking away blocks normally used for paging(PCH) and access grant(AGCH). Typically, System Information 7 and 8 messages are broadcast, however, types 5,13,16 and 17 can be broadcast. Since my network, Optus, does not use the BCCH Ext (most networks do not as it seriously reduces paging capacity), this counter is still 0 on this 2.5 year old phone. [GSM 05.02:6.3.1.3, 6.5.1(v), 7(table 3)]

These counters can only be reset with “Test 60 – Reset Counters”. The values are stored in the EEPROM, and are preserved across reboots, SIM card changes, and even software upgrades (provided the EEPROM is not cleared). Note, they are only saved when the phone is properly powered off, hence if the phone crashes or the battery is removed, the totals will not be updated.

Test 62 – Neighbour Measurement Information (33xx)

Available in: 3310, 2100, 3330, 7110

This test displays counters regarding measurements of neighbour cells.

```

62      21:11
PSW : 35121
SYNCR: 45984
BCCH : 24401
BCCHE: 0

```

```

62      Menu    21:11
PSW :
SYNCR:
BCCH :
BCCHE:
Menu

```

```

62      12:57
NeahrPswCtr
SyncMeasCntr
BCCHMeasAtmp
BCCHExtMeAtm
Menu

```

Red :

Green : The number of times (in decimal) the MS has synchronized to neighbouring BTS, as described in “Test 62 – Neighbour Measurement Information”

Blue : The number of times (in decimal) the MS has attempted to decode the BCCH information of neighbour cells, as described in “Test 62 – Neighbour Measurement Information”

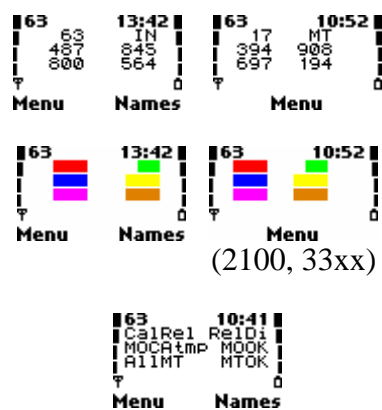
Yellow : The number of times (in decimal) the MS has attempted to decode the BCCH Ext information of neighbour cells, as described in “Test 62 – Neighbour Measurement Information”

This test is identical to “Test 62 – Neighbour Measurement Information”, however, the values are displayed in decimal.

Test 63 – Call Attempts Counters

Available in: 2100, 3310, 3330, 5110, 6150, 6210, 8210, 8250

This test displays the statistics for successful and failed dialed and received/missed calls, and the reason the last call was cleared.



Red : The reason the last call was cleared (disconnected). See “Test 39 – Reason for Last Call Release” for more information about this value. [GSM 04.08:F,G,H]

Green : Additional information about how the last call was cleared. Can be:

MT: Mobile Terminated – The network disconnected the call

MO: Mobile originated – one of the phones disconnected the call

IN: Internal – the call could not go ahead/was disconnected due to an internal problem (such as no coverage)

UN: Unknown – The reason is unknown. This is also displayed after power-on.

Blue : Number of dialled (MO) calls attempted (in decimal). This counter is increased whenever the call button is pressed to make a call.

Yellow : Number of successful dialled (MO) calls (in decimal). This counter is updated when the network delivers a CONNECT message. Note, when calling some other network (GSM, PSTN) this counter may be updated once the phone at the other end starts ringing, in other words, when the “Hold” function appears on the phone’s

screen. This is due to issues with some networks not properly signalling the MS, notably Optus.

Pink : Number of calls attempted to be received (MT) (in decimal) (this includes missed calls)

Orange : Number of successful received calls (in decimal). This counter is incremented when the call is answered. Hence it does not include missed calls.

The successful and attempted counters have a maximum display of 3 digits. This means you will only see the last 3 digits of the actual value, so after 999 it will appear to wrap around to 0.

It is then possible to calculate the number of failed attempts by subtracting the successful number from the attempted number, provided the counters have not wrapped around more than once. Note for the MT calls, the failed counters will include missed calls.

These counters can only be reset with “Test 60 – Reset Counters”. The values are stored in the EEPROM, and are preserved across reboots, SIM card changes, and even software upgrades (provided the EEPROM is not cleared). Note, they are only saved when the phone is properly powered off, hence if the phone crashes or the battery is removed, the totals will not be updated.

These counters are useful for determining how many calls you may have attempted/attempted/received during a period of time (you can reset them to start from 0, or remember the previous value and subtract that). These counters cannot really be used to dispute bills however, since they are technically alterable, and can be made not to update by disconnecting the battery. Nor do they necessarily show if a call was answered (see above).

Test 64 – Location Update Counters

Available in: 2100, 3310, 3330, 5110, 6150, 6210, 8210, 8250

This test displays counters on successful and failed location updates and IMSI attaches.

The image shows three screenshots of the Test 64 location update counters menu. The first two screenshots show the menu with data for menu items 0472, 0310, 0081, and 0635. The third screenshot shows the menu with colored bars for 'NFai', 'PFai', and 'Loc update counters'.

```

64 13:46 64 13:46
0 472 284 0081 035
0 310 285 0635 626
Menu Names Menu
Menu Names Menu
(2100, 33xx)
64 11:38
NFai NL NLOK
PFai PL PLOK
Loc update
counters
Menu Names
  
```

Red : The reason of failure of the last normal location update

Green : Number of attempted normal location updates (in decimal)

Blue: Number of successful normal location updates (in decimal)

Yellow : The reason of failure of the last periodic location update or IMSI attach

Pink: Number of attempted periodic location updates and IMSI attaches (in decimal)

Orange : Number of successful periodic location updates and IMSI attaches (in decimal)

[GSM 04.08:4.4]

Location updates are performed whenever the phone moves to a different LAC (this is known as a normal location update) (group of cells) in order to tell the network where it can be found (so the network can send page requests to the right group of cells).

They are also performed periodically (if the network operator chooses – you can find out more in “Test 10 – TMSI, PRP, T3212 (Location Update) timer and AFC/AGC Information”. IMSI attaches may also be required by the network operator (you can find out if IMSI attaches are used in “Test 07 – Current Cell Flags”). IMSI attaches are when the phone does a special type of location update when powered on, so the network knows that it is ready to receive calls and SMS messages.

Whenever the phone establishes a connection with the network, a location update is made implicitly (since the network obviously knows where the phone is).

These counters have a maximum display of 3 digits. This means you will only see the last 3 digits of the actual value, so after 999 it will appear to wrap around to 0.

The reasons of failure are described in “Test 39 – Reason for Last Call Release”, in the Mobility Management (MM) section, since location updating is an MM procedure.

This test can be used at the end of a trip to see how many times you have changed LAC – subtract the number of successful normal location updates from the initial value (before the trip), or reset the counters at the start of the trip.

These counters can only be reset with “Test 60 – Reset Counters”. The values are stored in the EEPROM, and are preserved across reboots, SIM card changes, and even software upgrades (provided the EEPROM is not cleared). Note, they are only saved when the phone is properly powered off, hence if the phone crashes or the battery is removed, the totals will not be updated.

Test 65 – SMS Counters

Available in: 2100, 3310, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays counters on successful and failed SMS messages.

```
65 21:53 0 502 438 0 759 748
Menu Names

65 11:54 0266 261 0390 390
Menu
```




Red : This value is the error code of the reason the last message failed to send. See below for a description of the error codes.

Green : This is a counter (in decimal) of the number of messages that the phone has attempted to send.

Dark Blue : This is a counter (in decimal) of the number of successful messages that have been sent.

Yellow : This value is the error code of the reason the last message failed to receive.

Pink : This is a counter (in decimal) of the number of messages that the phone has attempted to receive.

Orange : This is a counter (in decimal) of the number of successful messages that have been received.

Light Blue : This is a counter (in decimal) related to Cell Broadcast Schedule messages - additional details are unknown at this point. [GSM 04.12]

These counters, except for the cell broadcast counter, have a maximum display of 3 digits. This means you will only see the last 3 digits of the actual value, so after 999 it will appear to wrap around to 0.

The number of failed SMSs can be calculated by subtracting the number of successful messages from the number of attempted messages, in both receive and send counters, provided that neither counter has wrapped around more than once.

Note, these send/fail counters only operate at the SM RL (SMS Relay Layer). That is, a 'success' is when the message makes it to the MSC and through to the SC, not the recipient. Delivery reports (if enabled) confirm whether the SMS was actually delivered, however these counters do not read these, as delivery reports operate at the SM TL (SMS Transport Layer). Received delivery reports will show up as a successful received message.

These counters can only be reset with "Test 60 – Reset Counters". The values are stored in the EEPROM, and are preserved across reboots, SIM card changes, and even software upgrades (provided the EEPROM is not cleared). Note, they are only saved when the phone is properly powered off, hence if the phone crashes or the battery is removed, the totals will not be updated.

These counters can be useful for checking how many SMS messages you have sent (and received) which you can compare with your bill. Either reset the counters with Test 60 at the start of each month, or remember the last value. If you send more than 1000 messages each month you might also need to note overflows in the counter. If your carrier doesn't bill you for undelivered SMS messages these counters could be greater than that on your bill. Otherwise, they should closely match.

SMS error codes:

1 – Number not in use (send).

21 – Invalid number

22 – Phone/SIM memory is full (receive). Older phones store their SMS messages on the SIM card, which have varying capacity. Newer phones can also store messages on the phone.

38 – SMSC is blocked or invalid (send)

252 – Phone cannot find network (send)

[GSM 04.11:8.2.5.4]

SM AL (Application Layer), SM TL (Transport Layer) described in GSM 03.40

SM RL (Relay Layer), SMSC (Control Layer) described in GSM 04.11

Test 66 – SMS Relay/CM Layer Counters

Available in: 2100, 3310, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about timers associated with SMS messages at the SM-RL (Short Message Relay Layer) and SM CM (Short Message Connection Management) Layer.

```
66 13:04
 24 30 0 0
Menu Names

66 13:04
 24 30 0 0
Menu Names

66 13:13
TR1 TR2 TRA
TC1 TC2 SCH
SMS timeout
counters
Menu Names
```

Red : Number of TR1M timer expiries (in decimal). The TR1M timer controls how long the mobile station will wait for an (Relay Layer) acknowledgement (either error or success) from the network after it has submitted the TPDU (packet containing SMS and additional header information). If this timer expires, the Short Message Relay Layer will abort the connection. It is usually rare for this timer to expire, as normally at this layer a error is returned indicating the reason the SMS could not be sent. TR1M timeout can be between 35-45 seconds. [GSM 04.11:6.3.1,10.x]

Green : Number of TR2M timer expiries (in decimal). The TR2M timer controls how long the mobile station will wait for it's own upper layers to give it the signal to transmit an (Relay Layer) acknowledgement (either error or success) after receiving a TPDU. Expiry of this timer is also rare as it is a result of the mobile station upper layers taking too long to decode the TPDU. When this timer expires, the connection is aborted. TR2M timeout can be between 12 – 20 seconds. [GSM 04.11:6.3.1,10.x]

Blue : Number of TRAM timer expiries (in decimal). The TRAM timer controls how long the mobile station's Short Message Relay Layer will wait before reattempting (if

allowed) a “memory available for SMS notification” that has been rejected by the network due to TR1M timer expiry or temporary failure. TRAM timeout can be between 25-35 seconds. [GSM 04.11:6.3.3,10.x]

Yellow : Number of TC1 timer expiries (in decimal). The TC1 timer controls how long the mobile station’s Short Message Control Layer will wait for an acknowledgement (either error or success) from MSC to allow it do determine if the MSC accepted the message or not. (Note this is different to the acknowledgement associated with the TR1M timer which arrives later - the TC1 acknowledgement is generally associated with the physical radio connection, whereas the TR1M timer is associated with the SMS being accepted at higher layers). If the TC1 timer expires the mobile station can reattempt the data transfer up to 3 times. Generally, this is the timer to expire as radio link failures are more likely than errors in the SM Transport Layer. [GSM 04.11:5.3]

Pink : ?

Orange : Number of Cell-broadcast schedule message timeouts (in decimal). Likely to be the number of times the MS has given up listening on the CBCH (Cell-Broadcast Channel) waiting for SMSCB (SMS Cell Broadcast) schedule messages, which describe when the differing types of cell-broadcast message will be broadcast (in order for the MS to avoid having to continually listen and waste power). [GSM 04.12:2.1]

These counters can only be reset with “Test 60 – Reset Counters”. The values are stored in the EEPROM, and are preserved across reboots, SIM card changes, and even software upgrades (provided the EEPROM is not cleared). Note, they are only saved when the phone is properly powered off, hence if the phone crashes or the battery is removed, the totals will not be updated.

SM RL (Relay Layer), SMSC (Control Layer) described in GSM 04.11

17. Phone Software Information – Tests 80 – 89

Test 80 – Reset Timers (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test will reset the timers in “Test 82 – View timers” to zero.

```
80      09:50
┌───────────┐
│  TIMERS    │
│  RESET     │
└───────────┘
Menu      Names
```



```
80      12:39
┌───────────┐
│ Use menu   │
│ to reset  │
│ field test│
│ timers    │
└───────────┘
Menu      Names
```

Jumping to this test will clear the timers. The test will not display anything else, even after resetting.

Test 81 – Enable/Disable Timers (active)

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test will enable or disable the timers in “Test 82 – View timers”.



Red : Displays the status of the timers – “ENABLED” or “DISABLED”. Jumping to this test will toggle this state

This test does not reset the timers; when you disable the timers they are simply suspended with their current values, and will resume once timers are re-enabled.

The status of this test is stored in EEPROM; it is remembered across power off.

Test 82 – View timers

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250



Red : Time the phone has been powered on; this is not the time since the last reboot, but how long the phone has been powered up in total (see below)

Green : Time the phone has been logged into a network

Blue: How long the phone has been in the NSPS (No Service Power Save) state (no network)

Yellow: How long the transmitter has been on.

Pink : State of the timers – either “ON” or “OFF” (see “Test 82 – Enable/Disable timers”)

The format of the timers is 5 digits, the first 3 digits are hours, and the last 2 digits are minutes. So 02132 is 21 hours, 32 minutes. However the maximum value is 099:59 (99 hours 59 minutes). Once one of the timers reaches this value (usually the first), all other timers will stop until the timers are reset.

These timers only operate when timers are enabled (in Test 82), and a Net Monitor test is being displayed. These counters do not work when no Net Monitor tests are being displayed (Test 00).

These timers are preserved across a reboot, i.e. rebooting the phone does not clear the timers. Hence the timers show the total time across the phone's lifetime (or since last reset).

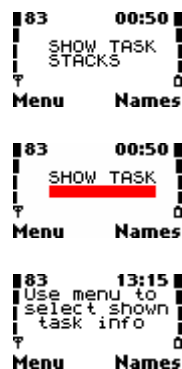
On the phones I have tested, a minute on the timers is a real life minute, however on the 7110 a minute on the counter is 30 seconds in real life, so you need to half the value on the counter.

These timers are reset to 0 with "Test 80 – Reset Timers". These timers are also reset if the charger is disconnected and the phone's battery is full. You can get around this possibly unwanted reset by powering off the phone, disconnecting the charger, and powering it back on (remember values are not cleared across reboot).

Test 83 – Change Information Shown in Tests 84-87 (active)

Available in: 2100, 3330, 5110, 6210, 7110, 8210, 8250

This test changes the type of information shown in "Test 84-87 – Task Information".



Red : Indicates the type of information shown for each task in "Tests 84-87 – Information about Tasks". Jumping to this test will cycle through "STACKS", "MSG BUFS" and "FAST BUFS".

In Tests 84-87 each value is associated with a task (which varies from phone model to model). A task is simply like a task on a computer, the phone's operating system too runs multiple tasks which do different things (e.g. SMS, monitoring network, infra-red, etc).

The meaning of the value is changed with this test. In other words, you can display three types of information about each task – peak stack usage, peak pending message buffers and peak pending fast message buffers.

The stack usage values indicate how much stack space (in bytes??) has been free in the worst case scenario (when the most stack was used). The stack is an area for each task to store temporary variables. Unlike most stacks in computers, which can grow, the stacks in the phone have a maximum allowed size. When the stack is full and more data is added (known as stack overflow) (although this is not supposed to happen), the phone software will reset and “Test 35 – Reason for Last Software Reset” will show “STACK” the next time the phone is turned on. These values will never increase, they will only decrease (as a new maximum amount of stack is used). For example, if you look at the IRDA task stack after turning the phone on, it will be a large value. After enabling infra-red, it will decrease further (more stack used), and after establishing a connection it will decrease even further.

Since these values are not saved across a restart, if a stack overflow occurs, “Test 57 – Stack and Memory status before Reset” will indicate which stack overflowed.

The message buffers are presumably referring to the inter process communication procedures used by the phone’s operating system software. Presumably, tasks communicate with each other by posting messages to each others message queues (in a similar way to applications that run on Microsoft® Windows®). There are two message queues, a normal and a fast. The fast is presumably checked first, as it would contain urgent or important messages, then the normal queue is checked. The peak pending message buffers and peak pending fast messages are referring to the maximum number of normal and fast messages (respectively) that have been in the respective queues so far. Hence, conversely to stack size, these values should never decrease, only increase (a new maximum number of message buffers are pending).

As mentioned before, these values are not stored in the EEPROM or anywhere else. Thus, they are lost on reset and start fresh on power on.

Test 84,85,86,87 – Information about Tasks

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

These tests display the requested information selected in “Test 83 - Change Information Shown in Tests 84-87”. The tasks will vary depending on phone and software version, so it is necessary to use the help screens.

```

  84      11:37 84      11:37 84      11:37 84      11:38
  00003  0324  0000  3  0  0  0  0  0  0  0  0  0  0  0  0  0
  00006  0724  0000  1  0  0  0  0  0  0  0  0  0  0  0  0  0
  00000  0000  0000  4  0  0  0  0  0  0  0  0  0  0  0  0  0
  2600  0000  0000  0  0  0  0  0  0  0  0  0  0  0  0  0  0
  Menu  Names Menu  Names Menu  Names Menu  Names
  
```

Each value in these tests displays information about a particular task. The task name can be found out by using the help screen, the task name will replace the value that represents that task. Each value is in decimal. See “5. How do I use Net Monitor?” for more information about help screens.

The type of information shown can be controlled with “Test 83 – Change Information Shown in Tests 84-87”, and will cycle through peak stack usage, peak pending message buffers, and peak pending fast message buffers.

These counters are not stored and are reset on a power on.

Test 88 – Information About Software Versions

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays information about MCU (Main Control Unit), PPM (Post Programmable Memory) and DSP (Digital Signal Processor) software versions.



Red : The version of the current (MCU) software. This can also be found out using the *#0000# code at the home screen.

Green : The version of the current PPM package – this contains the language packs and is different to each region. This is in the format of a number followed by a letter. The number should match the MCU version, and the letter indicates which PPM package it is, in this phone, package ‘D’ which has languages English, German and Portuguese. Those who flash phones will note this letter corresponds to the PPM packages.

Blue : The date of release of the MCU software. This can also be found using the *#0000# code at the home screen. Date is in the format yymmdd.

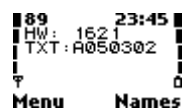
Yellow : The 16-bit checksum (4 hexadecimal digits) of the MCU software. The phone checks this on startup; if it does not match the calculated checksum, the phone displays “CONTACT SERVICE”.

Pink : The DSP version.

Test 89 – Information about Hardware and Text Version

Available in: 2100, 3330, 5110, 6150, 6210, 7110, 8210, 8250

This test displays the hardware and text version



```

89 23:45
HW: ██████████
TXT: ██████████
Menu Names

```

```

89 22:40
HW version
Text version
Menu Names

```

Red : Hardware version number. This matches the hardware version referred to in service manuals. It usually has a relation to the PCB (board) revision too, e.g. 1621 would correspond to RML7_16

Green : Text version – version of text in phone, such as languages and operator names. In the form of a date. with a letter preceding, i.e. Xddmmyy.

This test is useful for determining the hardware version, as it can allow you to identify how old the phone is (software date is not necessarily accurate due to upgrades), and also if the phone is capable of handling certain software (e.g. 8210s with hardware version 1903 or greater can be loaded with 8250 software).

18. Test 90 and onwards

Test 90 and onwards seem to be very phone specific and vary greatly from model to model. This information is largely specific to one specific function of the phone; such as voice dialling. As this information is about functions internal to Nokia software it is difficult to confirm and make sense of many of the parameters.

I have uncovered a considerable amount of information about these tests, and will eventually document them in future versions of this document, as I learn more about them. However, I will not endeavour to complete this section, as much of the information in these tests is not as useful as Tests 1 – 89.

Test 132 – Statistics about calls

Available in: 2100, 3310, 3330

This test displays statistics about calls made and received in the phone’s lifetime.

```

132 13:10
BS: 00000306
MO: 00000259
DRC: 00000002
TIM: 000199C1
Menu Names

```

```

132 13:10
BS: ██████████
MO: ██████████
DRC: ██████████
TIM: ██████████
Menu Names

```

```

132 13:11
BS_Call Cnt
MO_Call cnt
Dropped call
Call time
Menu Names

```


Red : ...

Green : ...

Blue : The number of calls (in decimal) that have terminated abnormally. I have been unable to full determine which types of failure cause this counter to increment, however it seems to include all Radio Link Failures (RLT reaches 0) and Handover failures.

Yellow :

19. Field Test (ftd) Symbian Application

19.1 Introduction

Unfortunately as of the last few years (the 8310 was probably the starting point), Nokia have removed the Net Monitor / Field Test functionality from their DCT-4 range of phones. At the same time, Nokia introduced GPRS into the 8310 and many subsequent phones. Consequently, a Net Monitor with extended GPRS tests was not easily available.

The Nokia 7650 was the exception to this. I'm not entirely sure on the details as to how it came about, but somehow a Ftd (Field Test) application for the Symbian OS appeared which added quite a few new interesting tests (which are documented in subsequent sections). Furthermore, because the 7650 has a nice large color display, the tests are less cluttered and easier to read.

19.2 Installing Ftd

From what I have been told, the Ftd application only runs on certain firmware versions. So far, I have successfully run it on v3.12, however it failed on v4.39.

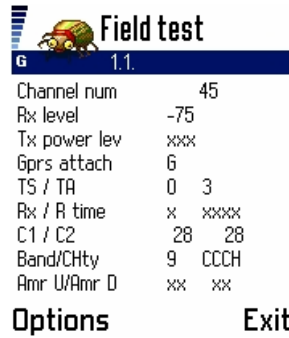
The installation of Ftd is now quite simple. Previously, it involved using a file manager to manually copy the various files to system directories. Now, it has been packaged as a self-installing SIS file that does it all for you.

Update: Unfortunately the previous URL is down. Try a search on the <http://www.nokiafree.org/forums>.

Now, simply send the "Net Monitor (Repack) (Vers. 1.00) (Full).sis" to the phone via Bluetooth or Infrared (you can even do this straight from Windows Explorer on Windows XP). Then, install the application in the usual manner by opening the .SIS file.

19.3 Using Ftd

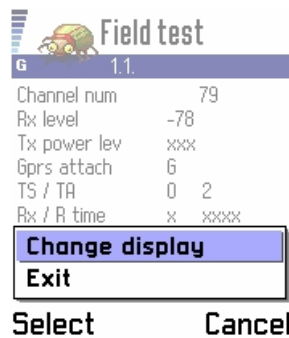
Ftd, like Net Monitor, is a series of tests which comprise a single screen, some of which are active (executable), some of which are view only. The tests are numbered at the top in the form 'x.y', where x is the test group and y is the test number within that group.



When you open the application you will find yourself at one of the test screens (normally 1.1). Moving around the test screens is simple using the stick. Moving the stick down will move to the next test. Similarly, moving the stick up will move to the previous test. At the end of a test group, navigation will ‘wrap around’ to the next test group. For example, the test after 6.9 (last test of group 6) is 7.1 (first test of group 7).

Moving the stick right or left will advance to the start of the next or previous test group, respectively. Pressing the stick will simply activate the LCD backlight (if not already activated).

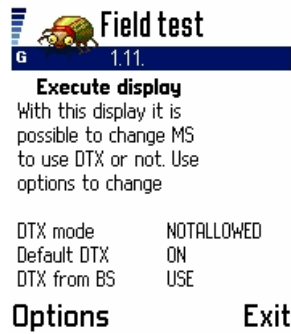
There is also an options menu which allows additional functions.



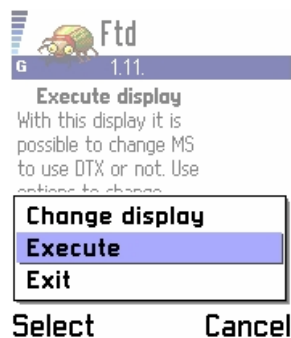
The ‘Change Display’ option simply prompts a dialog box where a quick jump to a known test can be entered. The format must be a 4 digit code, where the first 2 digits refer to the test group, and the last 2 digits refer to the test within that group. For example, Test 1.10 would be written as “0110”. Please note also, that unlike Net Monitor, jumping to an active test will not change anything. Active tests are handled a different way, as described next.

19.4 Active tests

Ftd, like Net Monitor includes active tests, where parameters for the test can be changed. Those tests that are active (executable) are usually indicated as being so by the text on the screen. For example, Test 1.11 looks like this:



In active texts, the options menu includes an additional item called “Execute”.



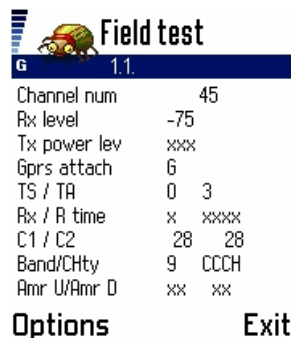
For active tests which have a ‘toggle/cycle’ style operation, choosing ‘Execute’ will simply invoke that toggle/cycle. For active tests where a value needs to be entered, a dialog box will appear where the value is to be entered. In Net Monitor, values were entered in a far less convenient way, by saving to SIM memory.

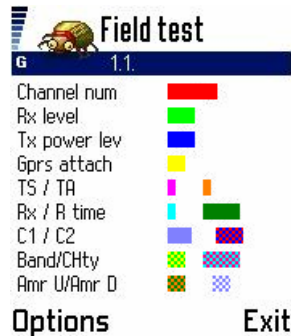
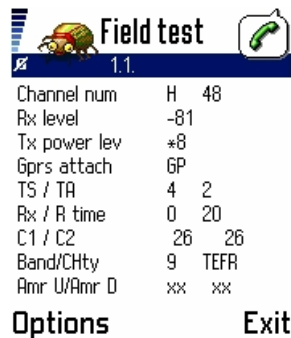
20. Field Test (ftd) – Group 1

Test 1.1 – Serving Cell Information (1)

Available in: 7650

This test displays information about signal, selection characteristics and communication with the serving BTS. It is continued in “Test 1.2 – Serving Cell Information (2)”





Red : Current ARFCN (Absolute Radio Frequency Channel Number) of serving cell. See Test 01.

Light Green : Signal strength of the serving cell, in dBm. See Test 01.

Dark Blue : Transmitter power level (or 'xxx' when idle). See Test 01.

Yellow: GPRS attach state. Displays 'G' if GPRS attached, and 'P' if GPRS-attached and a PDP context is activated.

Pink : Current timeslot number, 0-7 (0 if idle). See Test 01.

Orange : Current timing advance, 0-63 (or last timing advance, if idle). See Test 01.

Light Blue : RXQUAL_SUB value, 0-7 ('x' if idle). See Test 01.

Dark Green : Radio Link Timeout value, 4-64. (or 'xxxx' when idle). See Test 01.

Grey : Current C1 (path loss criterion) value, -99 – 999. See Test 01.

Red-Blue : Current C2 (reselection criterion) value, -99 – 999. See Test 01.

Green-Yellow : Current band of operation. '9' for GSM900, "18" for GSM1800

Light Blue-Pink: The type of logical channel or sub channel or codec/data rate the phone is currently using. See Test 01.

Orange-Dark Green :

Grey-White : Something to do with Adaptive Multi Rate (AMR) codec. Unable to test due to non-support in any Australian networks.

As it can be seen, this test is very similar to Net Monitor's Test 01. Most of the information about the fields can therefore be obtained from that test.

Test 1.2 – Serving Cell Information (2)

Available in: 7650

This test displays information about signal, selection characteristics and communication with the serving BTS.

Field test	
G	1.2
Paging mode	NO
max RACH retr	4
Roaming ind	
BSIC value	B43
CC Cause	16
Rx quality	x
CRD / Hopping	0 0
PenT / HCh	0 0
MAIO / HSN	xx xx
Options	Exit

Field test	
R	1.2
Paging mode	NO
max RACH retr	4
Roaming ind	
BSIC value	B24
CC Cause	16
Rx quality	0
CRD / Hopping	xxx xx
PenT / HCh	xxx 1
MAIO / HSN	0 6
Options	Exit

Field test	
G	1.2
Paging mode	■
max RACH retr	■
Roaming ind	■
BSIC value	■
CC Cause	■
Rx quality	■
CRD / Hopping	■ ■
PenT / HCh	■ ■
MAIO / HSN	■ ■
Options	Exit

Red : Current Paging Mode, NO/EX/RO/SB. See Test 02.

Green : Maximum RACH attempts, 1/2/4/7. See Test 02.

Dark Blue: Roaming indicator. “ “/R. See Test 02.

Yellow : BSIC value of current cell. See Test 02.

Pink : Call-Control Cause value (reason for last call termination). See Test 39.

Orange : The RXQUAL value. See Test 02.

Purple : Cell Reselect Offset, 0-126 (2dB steps). See Test 02.

Light Blue : Described as “Hopping”, but I believe this is actually the Temporary Offset (used to alter the C2 value when a cell is ‘new’). Temporary offset is in steps of 10dB from 0 to 70. A value of 70dB means ‘infinite’, i.e. the cell cannot be used during the time period. This value is only displayed in idle mode, otherwise ‘x’s are shown. See Test 02.

Dark Green : Penalty Time, in seconds, 0-620 (steps of 20). This value is only displayed in idle mode, otherwise ‘x’s are shown. See Test 02.

Grey : Indicates whether frequency hopping is used. Can be 0 (No) or 1 (Yes). Must always be 0 in idle mode. See Test 02

Red-Blue : Mobile Allocation Index Offset (MAIO), 0-63. See Test 02.

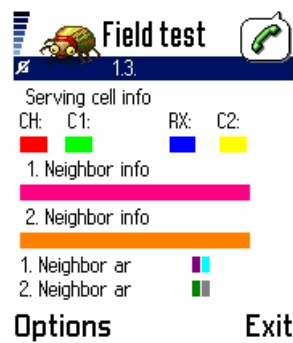
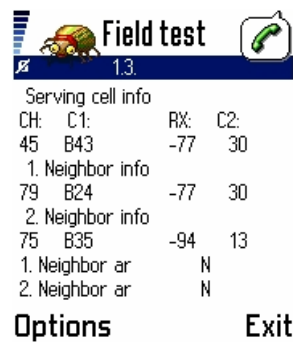
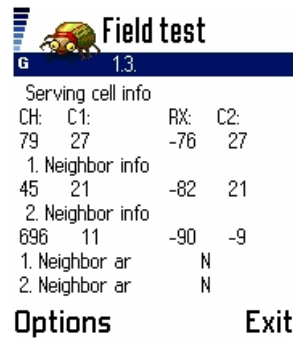
Green-Yellow : Hopping Sequence Number (HSN), 0-63. See Test 02.

See Test 02 for further information.

Test 1.3 – Selection characteristics of Serving Cell and Neighbour 1 and 2

Available in: 7650

This test displays a selection summary of the serving cell, and the 1st and 2nd neighbour cells.



Each cell is allocated it's own line in the display. The format of each line is identical.

Red : The radio channel number of the serving cell. See “Test 1 – Serving Cell Information (1)”. Note, for the serving cell only, unlike Test 3, this does not necessarily show the ARFCN of the BCCH carrier in dedicated mode. An ARFCN other than the BCCH ARFCN may be displayed if the ARFCN of the dedicated mode channel (i.e. SDCCH, TCH) is not the BCCH ARFCN. If hopping is enabled, this value will slowly cycle through the ARFCNs in the hopping sequence. [GSM 05.05:2.x]

Light Green : The C1 value of the serving cell in idle mode. See “Test 1 – Serving Cell Information (1)”. [GSM 05.08:6.4] In dedicated mode, this is the BSIC value used to distinguish between multiple cells using the same channel is shown, in the

form of a 2-digit value from 0-63 preceded by a 'B'. See "Test 2 – Serving Cell Information (2)". [GSM 03.03:A.1, 05.08:7.2]

Dark Blue : The received signal strength of the serving cell. This value is in dBm, but if the value is -100dBm or less, in order to fit the 3 digits, the '-' sign is not shown. [GSM 05.08:8.1]

Yellow : The C2 value of the serving cell in idle mode. See "Test 1 – Serving Cell Information (1)". If C2 values are not supported (see "Test 07 – Current Cell Flags"), the C1 value is displayed. Even if C2 values are supported, the C2 on many cells will equal the C1 value. In dedicated mode (i.e. call), normally the C1 value is displayed, unless the MS has not made a measurement or decoded sufficient information on the carrier's BCCH to calculate the C1 (it may display an incorrect value, or usually 100) [GSM 05.08:6.4]

Pink: A summary of information about the 1st neighbour cell. The format is exactly the same as the serving cell information (see above).

Orange : A summary of information about the 2nd neighbour cell. The format is exactly the same as the serving cell information (see above).

Purple : This indicates whether the 1st neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Light Blue : This indicates the selection priority of the 1st neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

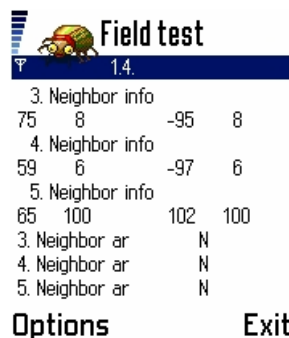
Dark Green : This indicates whether the 2nd neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Grey : This indicates the selection priority of the 2nd neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Test 1.4 – Selection characteristics of Neighbour 3, 4 and 5

Available in: 7650

This test displays a selection summary of the serving cell, and the 3rd, 4th and 5th neighbour cells.



The screenshot shows a mobile phone's field test interface. At the top, there is a signal strength indicator (four bars) and a small icon of a truck. The title "Field test" is displayed in a blue bar. Below the title, the text "1.4." is shown. The main content consists of three sections of neighbor information, each with four columns of data. The first section is for "3. Neighbor info" with values 75, 8, -95, and 8. The second section is for "4. Neighbor info" with values 59, 6, -97, and 6. The third section is for "5. Neighbor info" with values 65, 100, 102, and 100. Below these sections, there are three lines of "Neighbor ar" information, each with a value of "N". At the bottom of the screen, there are two buttons: "Options" and "Exit".

Test	1	2	3	4
3. Neighbor info	75	8	-95	8
4. Neighbor info	59	6	-97	6
5. Neighbor info	65	100	102	100
3. Neighbor ar				N
4. Neighbor ar				N
5. Neighbor ar				N

Field test			
1.4.			
3. Neighbor info			
75	B35	-88	19
4. Neighbor info			
43	B0	-97	10
5. Neighbor info			
47	B23	-98	100
3. Neighbor ar			N
4. Neighbor ar			N
5. Neighbor ar			N
Options		Exit	

Field test			
1.4.			
3. Neighbor info			
4. Neighbor info			
5. Neighbor info			
3. Neighbor ar			Yellow
4. Neighbor ar			Pink
5. Neighbor ar			Light Blue
Options		Exit	

Each cell has its own line. The format of each line is exactly the same as that of the serving cell (see Test 1.3).

Red : A summary of information about the 3rd neighbour cell.

Light Green : A summary of information about the 4th neighbour cell.

Dark Blue : A summary of information about the 5th neighbour cell.

Yellow : This indicates whether the 3rd neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Pink : This indicates the selection priority of the 3rd neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Orange : This indicates whether the 4th neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Purple : This indicates the selection priority of the 4th neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Light Blue : This indicates whether the 5th neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Dark Green : This indicates the selection priority of the 5th neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

These lines may not be displayed, if there are not enough cells to fill them, or if the BTS Test is enabled. Any line not displayed is shown as 'x's, including it's corresponding priority and forbidden indicator. See Test 1.3 for more information.

Test 1.5 – Selection characteristics of Neighbour 6, 7, and 8

Available in: 7650

This test displays a selection summary of the serving cell, and the 6th, 7th and 8th neighbour cells.

Field test			
1.5.			
6. Neighbor info			
65	100	104	100
7. Neighbor info			
xxx	xxx	xxx	xxx
8. Neighbor info			
xxx	xxx	xxx	xxx
6. Neighbor ar			N
7. Neighbor ar			x
8. Neighbor ar			x
Options		Exit	

Field test			
1.5.			
6. Neighbor info			
81	B54	-94	100
7. Neighbor info			
65	B3	101	100
8. Neighbor info			
59	B8	103	4
6. Neighbor ar			N
7. Neighbor ar			N
8. Neighbor ar			N
Options		Exit	

Field test			
1.5.			
6. Neighbor info			
7. Neighbor info			
8. Neighbor info			
6. Neighbor ar			█
7. Neighbor ar			█
8. Neighbor ar			█
Options		Exit	

Each cell has its own line. The format of each line is exactly the same as that of the serving cell (see Test 1.3)

Red : A summary of information about the 6th neighbour cell.

Light Green : A summary of information about the 7th neighbour cell.

Dark Blue : A summary of information about the 8th neighbour cell.

Yellow : This indicates whether the 6th neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Pink : This indicates the selection priority of the 6th neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Orange : This indicates whether the 7th neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

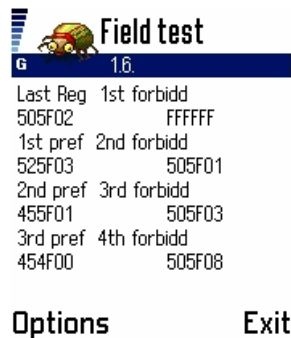
Purple : This indicates the selection priority of the 7th neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

Light Blue : This indicates whether the 8th neighbour cell is in a forbidden location. It displays 'F' if it is, otherwise it displays nothing.

Dark Green : This indicates the selection priority of the 8th neighbour cell. Can be 'N' (normal), 'L' (low), 'B' (barred). See below. [GSM 05.08:9.table1a, 03.22:3.5.1, 3.5.2]

These lines may not be displayed, if there are not enough cells to fill them, or if the BTS Test is enabled. Any line not displayed is shown as 'x's, including it's corresponding priority and forbidden indicator. Additionally, most Nokia models do not monitor the 7th and 8th neighbour cells in idle mode, as the GSM specifications only require 6 neighbour cells to be monitored. However they may do in dedicated mode. See Test 3 for more information.

Test 1.6 – Allowed and Forbidden Networks



Available in: 7650

This test displays information about the networks that you are allowed to use (or preferred when roaming is enabled) and forbidden to use.

Red : Last GSM Network the phone successfully registered to.

Green : First preferred alternate network.

Dark Blue : Second preferred alternate network.

Yellow : Third preferred alternate network

Pink : Forbidden network 1

Orange : Forbidden network 2

Purple: Forbidden network 3

Light Blue: Forbidden network 4

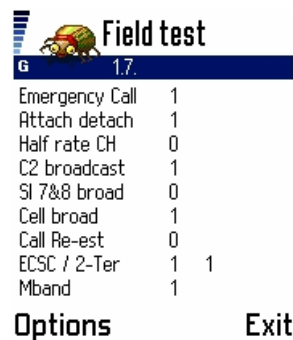
Please note, for 2-digit networks (most), due to the way this value is internally stored [GSM 04.08:10.5.1.3] with a nibble of 1s (0xF) prior to the two digits, the NCC part of the code will be shown as a 3-digit code with the first digit 'F'.

See Test 06 for further information.

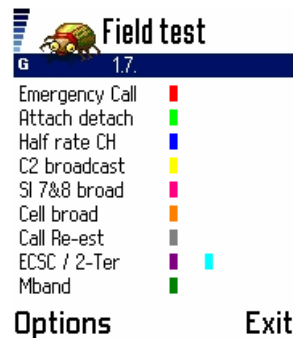
Test 1.7 – Current Cell Flags

Available in: 7650

This test displays values about the network and current cell, obtained from the current BTS.



Field test	
1.7.	
Emergency Call	1
Attach detach	1
Half rate CH	0
C2 broadcast	1
SI 7&8 broad	0
Cell broad	1
Call Re-est	0
ECSC / 2-Ter	1 1
Mband	1
Options	Exit



Field test	
1.7.	
Emergency Call	Red
Attach detach	Light Green
Half rate CH	Dark Blue
C2 broadcast	Yellow
SI 7&8 broad	Pink
Cell broad	Orange
Call Re-est	Grey
ECSC / 2-Ter	Purple
Mband	Dark Green
Options	Exit

Red : Emergency calls allowed (1=Yes, 2=No). See Test 07.

Light Green : IMSI-attach-detach procedure used. (1=Yes, 2=No). See Test 07

Dark Blue : Half rate traffic channels (TCHs) are supported (1=Yes, 2=No). See Test 07.

Yellow : C2 values are supported by the network (1=Yes, 2=No). See Test 07.

Pink : System Information (SI) messages 7 & 8 are broadcast by the cell (1=Yes, 2=No). See Test 07.

Orange : The network supports Cell Broadcast SMS messages (1=Yes, 2=No). See Test 07.

Grey : The network supports call-re-establishment (1=Yes, 2=No). See Test 07.

Purple : Early Classmark Sending (ECSC is supported (1=Yes, 2=No). Not displayed in dedicated mode ('x' is displayed instead). See Test 07.

Light Blue : System Information (SI) message 2Ter are broadcast by the cell (1=Yes, 2=No). Not displayed in dedicated mode ('x' is displayed instead). See Test 07.

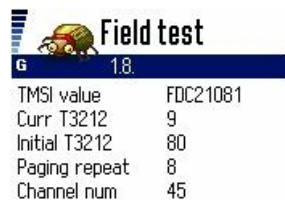
Dark Green : Multiband reporting - a value from 0-3 which decides how the dualband MS will report measurements to the network. See Test 07.

See Test 07 for further information.

Test 1.8 – TMSI, PRP, T3212 (Location Update) Timer Information

Available in: 7650

This test displays information about the state of the location update timer, the TMSI (Temporary Mobile Subscriber Identity) and the PRP (Paging Repeat Period).



Field test	
TMSI value	FDC21081
Curr T3212	9
Initial T3212	80
Paging repeat	8
Channel num	45

Options Exit



Field test	
TMSI value	
Curr T3212	
Initial T3212	
Paging repeat	
Channel num	

Options Exit

Red : Temporary Mobile Subscriber Identity (TMSI) – a unique 32-bit value represented in hexadecimal form. See Test 10.

Green : Current value of the T3212 timer, 0-240. See Test 10.

Dark Blue : Maximum value of the T3212 value, 0-240. See Test 10.

Yellow : Paging Repeat Period (PRP) value, 2-9. See Test 10.

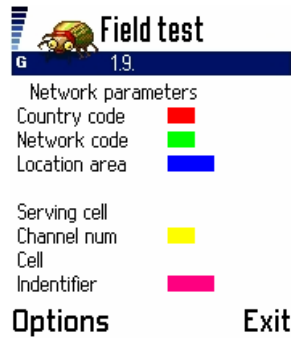
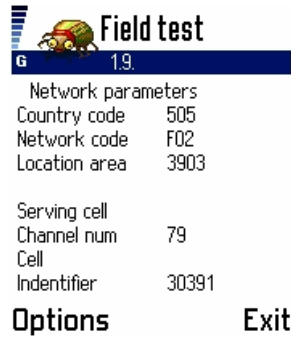
Pink : Channel – ARFCN of current serving cell. See Test 10.

See Test 10 for further information.

Test 1.9 – Cell and Local Area Information

Available in: 7650

This test displays basic information about the current cell and local area.



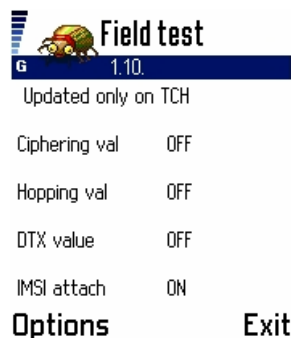
Red : Country Code (CC). 3-digit code to represent current country. See Test 11.
Green : Network Code (NC). Up to 3 digit network code of the current GSM network within the country. Please note, for 2-digit networks (most), due to the way this value is internally stored [GSM 04.08:10.5.1.3] with a nibble of 1s (0xF) prior to the two digits, the value will be shown as a 3-digit code with the first digit 'F'. See Test 11.
Blue : Location Area Code – 16-bit code (in decimal) of the current LA. See Test 11.
Yellow : Channel (Ch). Up to 4-digit code (10-bit) of the current cell's ARFCN (of BCCH). See Test 11.
Pink : Cell ID (CID) – 16-bit code (in decimal) of cell unique within LA. See Test 11.

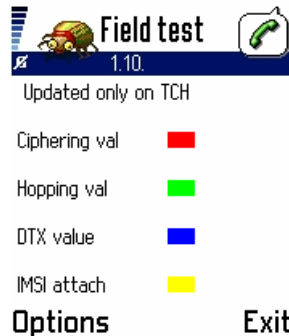
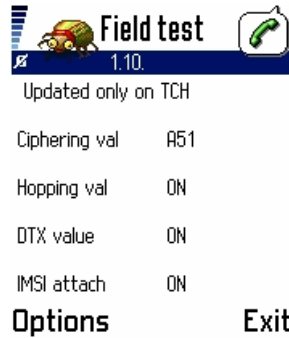
See Test 11 for further information.

Test 1.10 – Cipher (Encryption), Hopping, DTX and IMSI status

Available in: 7650

This test shows basic information about the encryption algorithm, whether hopping is used, whether DTX (discontinuous transmission) is used as well as the IMSI-attach-detach procedure is used. This information applies to the currently registered network, or the last registered network if the phone is not currently registered to a network





Red : Ciphering algorithm for Circuit Switched Connection. Can be A53, A52, A51 or “OFF”. This value is only displayed when the phone is communicating with the network (on a TCH), when idle this value is displayed as “OFF”. See Test 12.

Green : Displays whether frequency hopping is used or not (if on a TCH). Can be “ON” or “OFF”. See Test 12.

Blue : Displays whether DTX is used or not (if on a TCH) – can be “OFF” or “ON”. See Test 12.

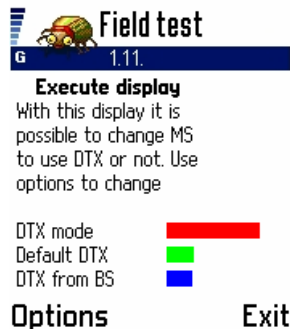
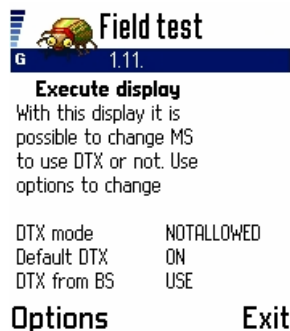
Yellow : Displays whether the IMSI-attach-detach procedure is used. Can be “ON” or “OFF”. See Test 12.

See Test 12 for further information.

Test 1.11 – DTX mode status / toggle (active)

Available in: 7650

This test allows you to view the DTX (Discontinuous transmission) mode which controls whether the transmitter is switched off when not necessary to save power (i.e. when phone user is not speaking). It also allows the mode to be toggled on or off if the BTS allows it.



Red : Displays the status of DTX mode. Can be “DTX:ON” (in use), “DTX:OFF” (not in use), “DTX:DEF” (uses default – see next) or “NOTALLOWED” (BTS decides, not MS). If the BTS allows it (see Test 13), choosing ‘Execute’ from the Options menu will cycle the mode.

Green : MS’s default DTX mode – this is what is used if DTX Mode (above) is set to “DTX:DEF”. Can be “ON” or “OFF”.

Blue : What the BTS says to use (on BCCH(SI3) or SACCH(SI6)) – can be “USE” (must be used), “NOT” (must not be used) or “MAY” (MS can decide)

See Test 13 for further information.

Test 1.13 – Change Behaviour for Barred Cells (active)

Available in: 7650

This test allows the user to allow the phone to ignore barred cells, or use only barred cells.





Red : Displays how the phone will respond to cell barring - values are “ACCEPTED”, “REVERSE” or “DISCARD”.

Choosing execute from the options menu of this test will cycle through “ACCEPTED”, “REVERSE” and “DISCARD”. Viewing this test will show the current behaviour in relation to barred cells.

Although the test describes it as “call bearer” instead of “cell barr”, it is most likely an error on behalf of the programmer/engineer who wrote this test.

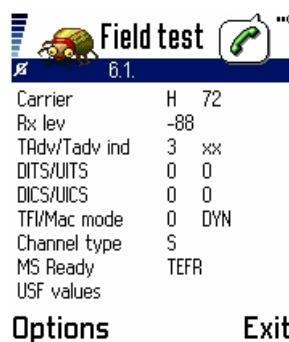
See Test 19 for further information.

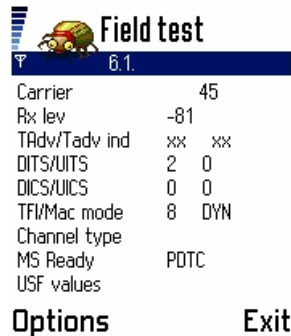
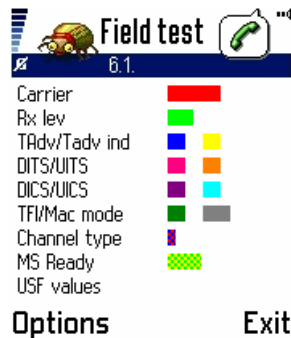
21. Field Test (ftd) – Group 6

Test 6.1 – General GPRS RLC/MAC information

Available in: 7650

This test displays general information about the RLC/MAC layer of the GPRS system.





Red : The current ARFCN used for transmission/reception. If hopping is used, a ‘H’ is displayed in front of the channel. In idle mode, provided the MS is both IMSI and GPRS attached, this will be the same value as in Test 1.1. This value is not displayed (appears as ‘x’s) when not GPRS attached. [GSM 05.02]

Light Green : The current received signal strength of the serving cell’s (measured on BCCH/PBCCH) in dBm. This value is not displayed (appears as ‘x’s) when not GPRS attached.

Dark Blue : The current (TA) Timing Advance value used by the mobile station. Shows ‘xx’ when not in a TBF or dedicated connection. Value is in GMSK symbol periods, from 0 to 63. This value is not displayed (appears as ‘x’s) when not GPRS attached. [GSM 05.10]

Yellow : The Timing Advance Index value, in decimal. The TAI is optionally assigned on the PACKET DOWNLINK ASSIGNMENT or PACKET UPLINK ASSIGNMENT and is used by the MS to perform the optional continuous timing advance update procedure. This procedure is useful if the MS is going to be in certain conditions where it is not likely to transmit data often (and hence the TA value calculated by the network will be more ‘rough’). This value refers to a particular PTCCCH sub-channel on the PDCH which will be used to transmit access bursts to allow the network to estimate the TA. The TAI is a 3-bit value between 0-7, or ‘x’ if the continuous update procedure is not used. [GSM 03.64:6.5.7, GSM 05.10:6.5.2]

Pink :

Orange :

Purple :

Light Blue :

Dark Green : Temporary Flow Identifier (TFI), in decimal. The TFI is used to identify a unique transaction to a particular Mobile Station on the PDCHs it is assigned (since the medium can be shared amongst multiple mobile stations). The TFI is included on both uplink and downlink data blocks and downlink control blocks. The TFI is a 5-bit value assigned by the network, and ranges from 0-31. [GSM 03.64:6.6.4.3, GSM 04.60:5.2.2, 7,8,9]

Grey : MAC (Medium Access Control) mode. This value decides how the MS will use the uplink (and share it with other possible MSes). Possible modes are “DYN”, “FIX?” and “EXT?”. The meaning of each mode is as follows:

Mode	Meaning
Fixed	The MS is assigned a bitmap of uplink radio blocks which it is allowed to use for the connection.
Dynamic	The MS is assigned blocks to transmit on dynamically by monitoring the Uplink State Flag on each timeslot it is assigned a USF.
Extended Dynamic	The MS is assigned blocks to transmit on dynamically by monitoring the Uplink State Flag on each timeslot it is assigned a USF. When it's USF occurs on a timeslot, it is allowed to transmit 1 or 4 radio blocks on that timeslot plus all higher numbered timeslots.

[GSM 04.60:5.2.4,8.1.1]

Red-Blue : Unclear what this parameter represents. It seems the help fields for this and the next test have been accidentally reversed, and this field is described as “MS-Ready”. From what I've seen, it simply seems to indicate that last time of connection – “R” for GPRS TBF and “S” for CSD connection.

Green-Yellow : The channel type or voice codec used. This can be of the type specified in Test 01, or it can be of the additional GPRS types:

Channel Type	Description
PCCC	Listening to PCCCH paging messages and PBCCH
PDTC	Packet Data Traffic Channel – used to carry user data (i.e. LLC traffic) or control blocks.
PRAC	Packet Random Access Channel – used for Packet Channel Requests.
PAGC	Packet Access Grant Channel – used to assign packet downlink resources.

Please note if PCCCH is not available (see Test 6.6) many of these types will not be displayed. [GSM 05.02:3]

Test 6.2 – Uplink TBF establishment information

Available in: 7650

This test displays information about the procedure the MS will use to request an Uplink Temporary Block Flow (TBF).

Field test	
6.2	
UL TBF establishment	
Estab cause	ONE-PHASE
Channel req	RACH
Result of TBF	OK
Access type	1-PHASE
Radio prior	0

Options Exit

Field test	
6.2	
UL TBF establishment	
Estab cause	█
Channel req	█
Result of TBF	█
Access type	█
Radio prior	█

Options Exit

Red : The establishment cause that will be sent to the network. The establishment cause shall either be ONE-PHASE or TWO-PHASE. Both types are supported on both CCCH and PCCCH. In a TWO-PHASE packet access, the network assigns a small resource to use as a response to CHANNEL REQUEST. The MS is then required to send a PACKET RESOURCE REQUEST to request further resources. In a ONE-PHASE access, the resources are immediately assigned to the MS by the network. [GSM 04.60:7]

Green : The channel used for Packet Channel Request messages. Can be “RACH” – Random Access Channel on CCCH is used, or “PRACH” – Packet Random Access Channel on PCCCH is used. If the PCCCH is not present (See Test 6.6) then the only value can be “RACH”. This value may also depend on the Network operation mode (See Test 6.3). [GSM 04.60:7]

Blue : Result of the last TBF – whether it aborted normally or abnormally. Value can be “OK” (if the TBF succeeded and was released normally by the network) or “FAIL?” (if the TBF was released abnormally by the network or a timer expired waiting for response from the network). [GSM 04.60:7]

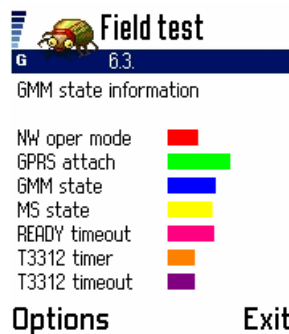
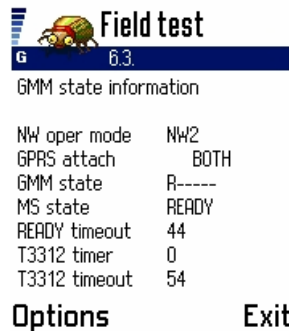
Yellow : Access Type – the type of access that will be used (1-PHASE for single phase access and 2-PHASE for two phase access). See above. [GSM 04.60:7]

Pink : Radio Priority. The radio priority that will be used for TBFs. This value appears to be chosen by the MS. The radio priority is used to decide how LLC PDUs will be ordered across the radio link (obviously higher radio priority takes precedence where possible). The radio priority is a 2-bit or 3-bit value (internal representation varies) where 0 is the highest priority (radio priority 1) and 3 is the lowest priority (radio priority 4) [GSM 04:08:10.5.7.2 GSM 04.60:7,8,9]

Test 6.3 – GMM state information

Available in: 7650

This test displays information about the GPRS Mobility Management (GMM) layer (in the MS).



Red : Network operation mode, as broadcast in GPRS Cell options IE either in BCCH (SI13 message) or PBCCH (PSI1/PSI13). [GSM 04.60:12.24] The network mode of operation decides whether Routing Area Updates will be performed independently of IMSI attaches and standard Location Area Updates (for GPRS & IMSI attached MSes). Values are “NW1”, “NW2” and “NW3”, which correspond to the 3 modes of network operation. In mode 1, when the RA or LA changes a combined update is sent through GPRS. In modes 2 & 3 (which are similar), updating is generally performed individually (RA updates through GPRS, LA updates via regular procedure). This value is subject to change from cell to cell. [GSM 04.08:4.7.2-5]

The network operation modes also define how paging is carried out. For mode 1, both GPRS/CS paging happens on the same paging channel (either PPCH/CCCH/PDCH) (paging is coordinated by the network). For mode 2, GPRS/CS paging happens on the CCCH. Mode 3 is similar to mode 2, but also allows paging on the PPCH (if supported). [GSM 03.60:6.3.3.1]

Green : Displays status of IMSI/GPRS attach. If the MS is not GPRS attached, “xxxxx” is displayed. If the MS is both GPRS and IMSI attached, “BOTH” is displayed. If the MS is only GPRS attached, “?” is displayed. [GSM 03.60:6.3]

Blue : GMM State. Displays “D-----“ if GPRS-detached, or “R-----“ if GPRS attached. [GSM 03.60:6.2]

Yellow : MS state. Can be “STAND” (for STANDBY) or “READY”. In the READY state, the MS is known at the individual cell level and the network or phone perform cell reselection (dependent on network settings). In the STANDBY state, the MS is known at Routing Area level. Transition from STANDBY to READY occurs on receipt or transmission of LLC frames. Transition from READY to STANDBY occurs on expiry of READY timer, when forced by the network or if radio problems

exist. This value is not displayed (appears as 'x's) when not GPRS attached. [GSM 03.60:6.1]

Pink : READY timer. The number of seconds of no LLC activity before the MS will return to the STANDBY state. This value is negotiated at GPRS-Attach or Routing Area Update. The maximum value is 192 minutes (11520 seconds). [GSM 04.08:4.7.2.1]

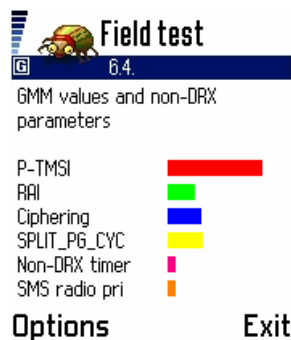
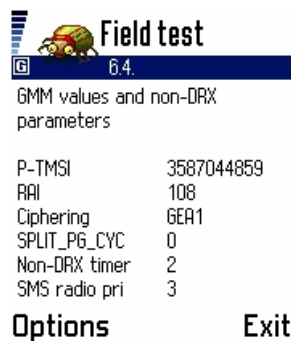
Orange : Value of the T3312 timer, in minutes. This timer controls how long after the MS has entered STANDBY state until the next periodic Routing Area update. When it reaches the T3312 timeout (see next), a RA update is performed. If the MS goes into READY and then back into STANDBY, the timer is reset (since the network now implicitly knows the RA). [GSM 04.08:4.7.x]

Purple : Value of the T3312 timeout, in minutes. The maximum value is 192 minutes (11520 seconds). See previous.

Test 6.4 – GMM values and non-DRX parameters

Available in: 7650

This test displays additional values about the GMM (GPRS Mobility Management) layer as well as some of the non-DRX parameters of the RLC/MAC/GMM layers.



Red : Current value of the P-TMSI. The P-TMSI is much like the TMSI, it is used to identify the MS temporarily and may be changed by the network. The P-TMSI is a 32-bit value represented in decimal, and thus ranges from 0 to $(2^{32}-1)$. [GSM 04.08:10.5.2.42]

Green : Current value of the RAI (Routing Area Identity). The RAI is much like LAC, it is a code assigned to 1 or more cells to which the MS is known to be listening to. The RAI is an 8-bit value represented in decimal, and thus ranges from 0 – 255. It is broadcast on BCCH (SI13) or PBCCH (PSI13). [GSM 03.03:4.2, GSM 04.08:10.5.5.15,4.7.x]

Blue : Current ciphering algorithm. In GPRS, ciphering is performed for the LLC layer, for traffic between the MS and the SGSN. The BSS is not involved in the ciphering procedure. The ciphering algorithm can either be GEA1 or OFF (no ciphering). [GSM 03.60:4.8, GSM 04.08:10.5.5.3]

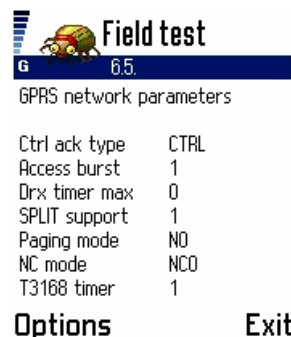
Yellow : Value of the SPLIT_PG_CYCLE parameter, in decimal. The SPLIT_PG_CYCLE parameter decides how often the MS will examine the PPCH (packet paging channel) or PCH for paging messages belonging to it. If PCH is used then if this value is greater than 32 it shall be limited to 32. This value ranges from 1 to 352 with the larger value indicating larger DRX (sleeping) times. If the value is 0, it is equivalent to no DRX (i.e. the MS constantly listens to paging channel). Not all Mobile Stations support SPLIT_PG_CYCLE on CCCH, hence the value may be 0. Not all networks support SPLIT_PG_CYCLE on CCCH either (see Test 6.5). The SPLIT_PG_CYCLE is requested by the MS on GPRS attach or RA update [GSM 03.64:6.5.10, GSM 04.08:5.5.1.5,10.5.5.6 GSM 05.02:6.5.6]

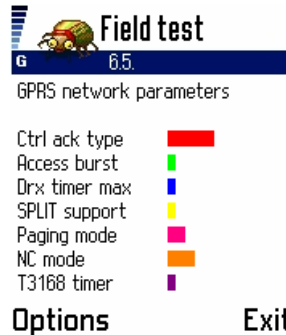
Pink : Value used to calculate the Non-DRX timer. When the MS returns to packet idle mode (i.e. after a TBF) it shall not enter DRX mode for the time period specified by the Non-DRX timer (i.e. it shall keep listening to all PCCCH/CCCH) blocks. The Non-DRX timer is calculated from the 3-bit value as follows (let 'x' be the value). Then, Non-DRX timer = $2^{(x-1)}$ seconds. In the case of x being zero, the value is 0 seconds (and hence the MS immediately enters DRX mode (if used) after a TBF). The Non-DRX period is requested by the MS on GPRS attach or RA update. [GSM 03.64:6.5.10, GSM 04.08:10.5.5.6, GSM 04.60:5.5.1.5]

Orange : SMS Radio Priority. The SMS Radio Priority decides the radio priority to be used for the sending of SMS messages over the GPRS network (i.e. via the SGSN). This value is sent by the network at GPRS attach. Not all networks support SMS via the SGSN, but this value is sent anyway. The radio priority is used to decide how LLC PDUs will be ordered across the radio link (obviously higher radio priority takes precedence where possible). The radio priority is a 2-bit or 3-bit value (internal representation varies) where 0 is the highest priority (radio priority 1) and 3 is the lowest priority (radio priority 4) [GSM 04:08:10.5.7.2 GSM 04.60:7,8,9]

Test 6.5 – GPRS Network Parameters

This test displays further information about parameters used by the RLC/MAC protocol.





Red : CONTROL_ACK_TYPE parameter. This is a single-bit flag broadcast on the PBCCH(PSI1/PSI13) or BCCH (SI13) to indicate what type of method to use to transmit PACKET CONTROL ACKNOWLEDGEMENT messages on the uplink. If the value is “4ACC”, 4 access bursts will be transmitted to carry the message; if the value is “CTRL”, the message will be transmitted as an RLC/MAC block. The network can override this parameter in the PACKET POLLING REQUEST message. The network might want the 4 access bursts to be sent as this allows it to calculate the MS’s timing advance more easily. [GSM 04.60:8.6, 11.2.2,12.24]

Green : ACCESS_BURST_TYPE parameter. This is a single-bit flag broadcast on the PBCCH(PSI1/PSI13) or BCCH(SI13) to indicate what type of bursts to use for access bursts (which are used on the PRACH, PTCCH and PACKET CONTROL ACKNOWLEDGEMENT message (if applicable – see above)). If the value is 0, the 8-bit access burst will be used. If the value is 1, the 11-bit access burst will be used. [GSM 04.60:12.24, GSM 05.03:5.3]

Blue : Value used to calculate DRX_TIMER_MAX. This is a 3-bit value broadcast on the PBCCH(PSI1/PSI13) or BCCH(SI13) to tell the MS the maximum value of the Non-DRX timer it can use (See Test 6.4). The value of DRX_TIMER_MAX in seconds is calculated as follows (let ‘x’ be the 3-bit value). Then $DRX_TIMER_MAX = 2^{(x-1)}$. Interestingly, I have seen the 7650 use higher values than this as the Non-DRX timer – perhaps firmware bug? [GSM 03.64:6.5.10, GSM 04.60:5.5.1.5]

Yellow : SPLIT support value. This value is a single bit flag broadcast on PBCCH(PSI13) or BCCH(SI13) to indicate whether SPLIT_PG_CYCLE (i.e. DRX) is supported on the CCCH in the cell. Values can be 0 (not supported) or 1 (supported). [GSM 04.08:10.5.2.37b]

Pink : Current Paging Mode. This is a 2-bit value broadcast on PBCCH(PSI1/PSI2/PSI3/PSI13) or BCCH(SI13) or in the last PACKET PAGING REQUEST/PAGING REQUEST message. Can be NO/EX/RO/SB. The meaning of the values are as follows:

Paging Mode	Meaning
NO – Normal Paging	The MS shall listen to its standard paging blocks at the times decided by its DRX settings
EX – Extended Paging	The MS shall also listen to possible paging messages in the 3 rd PCH block period on the PCCCH relative to its usual paging blocks. It shall also listen to its usual paging blocks
RO – Paging Reorganisation	The MS shall listen to all messages on the PCCCH and PBCCH
SB – Same as Before	The MS shall not change its paging mode

These values only apply in packet idle mode (i.e. no TBF exists). This MS changes its mode to the paging mode broadcast in the last paging message it received. This is why the “SB” mode exists – so the MS will keep its original paging mode (NO/EX/RO). If the PCCCH does not exist, this value will be the CCCH paging mode, see Test 02. [GSM 04.60:5.5.1.6,12.20]

Orange : NETWORK_CONTROL_ORDER parameter. This is a 2-bit value broadcast on the PBCCH(PSI5) or BCCH(SI13), or, it can be ordered by the network in other types of messages (PACKET CELL CHANGE ORDER and PACKET MEASUREMENT ORDER). The value can be “NC0”, “NC1” or “NC2”, corresponding to modes 1, 2 and 3 respectively. This value decides how the mobile station will send measurement reports and reselect cells when in the GPRS ACTIVE state (See Test 6.3). This does not affect GPRS STANDBY state. The modes can be summarized as follows:

NETWORK_CONTROL_ORDER	Meaning
0	The MS reselects cell as it does in STANDBY state.
1	The MS reselects cell as it does in STANDBY state, but is also required to submit measurement reports.
2	The network orders the cell reselection based upon information received in measurement reports submitted by the MS. The MS only performs cell reselection on events like downlink signalling failure (See Test 10) or Random access failure

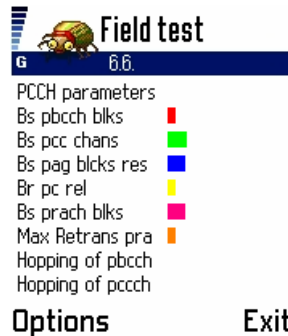
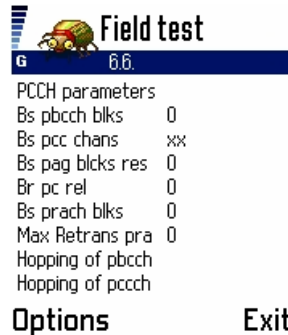
[GSM, 04.60:5.6.1, GSM 05.08:10.1.4]

Purple : The T3168 timer value. This value is a 3-bit value broadcast on the PBCCH(PSI1/PSI13) or BCCH(SI13). The T3168 timer controls how long the MS will wait for a PACKET UPLINK ASSIGNMENT message after requesting an uplink resource. If the timer expires, the MS considers the connection attempt to have failed. The T3168 timer has a value from 0-7, and the time period is calculated as (let ‘x’ be the value) 0.5(x+1) seconds. [GSM 04.60:7.1,12.24,13.1]

Test 6.6 – PCCCH parameters

Available in: 7650

This test displays information about the PCCCH (Packet Common Control CHannel), if allocated in the cell. The PCCCH is used like the CCCH, however is used to keep the GPRS MSes separate from the non-GPRS MSes (that way, the CCCH can be optimized for non-GPRS use). Not all networks and phones support the PCCCH (in fact, to enable it on some Nokia phones, the code *7220# (*pcc0#)). If the PCCCH is not available in the current cell, all values in this test will be 0, blank or ‘x’.



Red : BS_PBCCH_BLKs parameter, in decimal. This is a 2-bit value broadcast on the PBCCH (in PSI1) to indicate the number of blocks in the PDCH carrying the PBCCH. Values are from 0-3, which is 1 less than the actual number of blocks (i.e. 0 means 1 block, 1 means 2 blocks, etc). [GSM 04.60:12.25]

Green : BS_PCC_CHANs parameter, in decimal. This value indicates the number of PDCHs (i.e. timeslots on the PBCCH carrier) that carry PCCCHs. This value can be from 0-8, where 0 indicates there is no PCCCHs and hence no PBCCH, and that the remaining information in this test is irrelevant. This information is broadcast implicitly on PBCCH (PSI2). [GSM 05.02:3.3.2.4.1, GSM 04.60:11.2.19]

Blue : BS_PAG_BLKs_RES parameter, in decimal. This is a 4-bit value broadcast on the PBCCH (in PSI1) to indicate the number of blocks in the PDCHs used for the PCCCH that are to be reserved for PAGCH, PNCH, PDTCH and PACCH. Valid values are 0-12. [GSM 04.60:12.25]

Yellow : BS_PCC_REL parameter. This is a single bit flag broadcast on the PBCCH (in PSI1) to indicate if the PCCCH is going to be released shortly, and that all MSes listening to it should return to the CCCH/BCCH. GPRS allows the PCCCH to be created and destroyed dynamically, depending on changing network conditions. If the value is 1, the PCCCH will be released shortly. If the value is 0, the PCCCH will not be released for the time being. [GSM 04.60:12.25]

Pink : BS_PRACH_BLKs parameter, in decimal. This is a 4-bit value broadcast on the PBCCH (in PSI1) to indicate the number of blocks in a PDCH carrying PCCCH reserved for PRACH. Valid values are 0-12. [GSM 04.60:12.25]

Orange : The MAX_RETRANS parameter for PRACH. This parameter decides the maximum number of retransmissions of the PACKET CHANNEL REQUEST message allowed on the PRACH. It is (an array of 4) 2-bit values broadcast on PBCCH (in PSI1) – one value for each of the 4 different Radio Priorities. Only 1 value is shown here (?which radio priority?). The meaning of the value is as follows:

MAX_RETRANS	Maximum number of transmissions
0	1
1	2

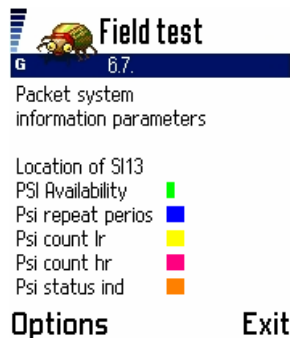
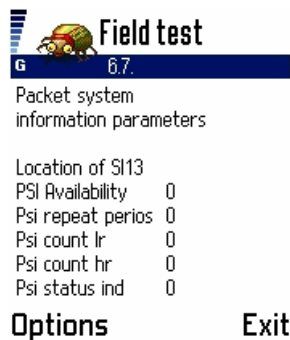
2	4
3	7

[GSM 04.60:7.1.2.1.1, 12.14]

Test 6.7 – Packet System Information parameters

Available in: 7650

This test displays information about PSI messages and how they are broadcast on PBCCH.



Red :

Green : PSI Availability – this value indicates whether the PCCCH (and hence PBCCH and PSI messages) exist. If the PCCCH does not exist, the value is 0. If the PCCCH exists, the value is 1. Could be PBCCH_CHANGE_MARK or PSI_CHANGE_FIELD??

Blue : PSI1_REPEAT_PERIOD value, in decimal This is a 4-bit value broadcast on BCCH(SI13) or PBCCH(PSI1/PSI13) or from a neighbour's PBCCH(PSI3/PSI3bis). The value indicates the number of 52-multiframes (PDCH blocks) between occurrences of the PSI1 message. It also indicates the cycle size of all the PSI messages, since all PSI messages must occur between occurrences of the PSI1 message. The value can range from 1-16 (or 0, if PCCCH does not exist). [GSM 04.60:11.2.18, GSM 05.02:6.3.2.4]

Yellow : PSI_COUNT_LR value, in decimal. This is a 6-bit value broadcast on the PBCCH(PSI1). This value indicates the number of PSI messages that are broadcast on the PBCCH with a low repetition rate. These messages are transmitted during the PSI1_REPEAT_PERIOD after the network has sent the PSI message and the PSI_COUNT_HR messages. [GSM 04.60:11.2.18, GSM 05.02:6.3.2.4]

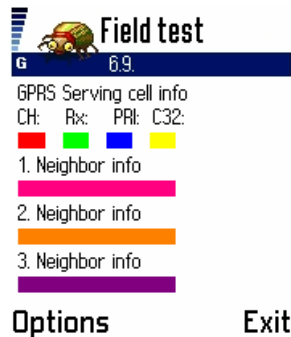
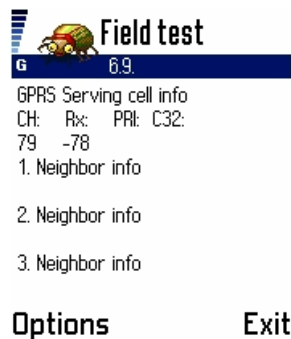
Pink : PSI_COUNT_HR value, in decimal. This is a 4-bit value broadcast on the PBCCH(PSI1). This value indicates the number of PSI messages that are broadcast on the PBCCH with a high repetition rate. These messages are transmitted during the PSI1_REPEAT_PERIOD after the network has sent the PSI1 message. [GSM 04.60:11.2.18, GSM 05.02:6.3.2.4]

Orange : PSI_CHANGE_FIELD or PBCCH_CHANGE_MARK??

Test 6.9 – GPRS Serving cell and neighbour information

Available in: 7650

This test displays information about the current GPRS serving cell and selection characteristics, as well as the neighbour cells. Much of this information may not be available if the phone is selecting cells by the C1/C2 method.



Red : Current ARFCN carrying the serving cell’s BCCH or PBCCH (if PCCCH used in cell), in GPRS-idle mode. Displays ‘xxxxx’ when GPRS-detached. If in dedicated mode, this displays the current ARFCN used, and may slowly rotate through the hopping sequence if hopping is used. Similarly, if a TBF exists, this may display the ARFCN used for the current TBF. [GSM 05.05:2.x]

Green : Receive signal strength of the serving cell, in dBm. If the value is smaller than -99dBm, the negative (‘-’) sign is not shown. (i.e. -103dBm is shown as 103).

Blue : Priority of the current cell (PRIORITY_CLASS), in decimal. This value will not be displayed if selecting using C1/C2 procedure. The PRIORITY_CLASS is a 3-bit value sent on the serving cell’s PBCCH (PSI 3) or a neighbour cell’s PBCCH(PSI3/PSI3bis) or in a PACKET MEASUREMENT ORDER message or PACKET CELL CHANGE ORDER (for MSeS in network control order mode 2) message. The PRIORITY_CLASS is from 0-7, with 7 being the highest priority. The PRIORITY_CLASS is used for two purposes. In calculating a neighbour C32 value, the TEMPORARY OFFSET is not applied if the neighbour cell’s priority class is

different from the serving cell's priority class. Secondly, when selecting a new cell, cells that have higher PRIORITY_CLASS take precedence. [GSM 04.60:11.2.20, GSM 05.08:10.1.2,10.1.3,10.4]

Yellow: C31 value of the current cell. The C31 value is calculated as the number of signal strength units (in dBm) greater than the HCS_THR value for that particular cell. For neighbour cells, the C31 also has an optional Temporary Offset applied for length Penalty time, similar to the C2 value (See Test 02). This value will not be displayed if selecting using C1/C2 procedure. [GSM 05.08:10.1.2,10.1.3]

Pink : Information about the 1st neighbour cell the MS is monitoring. This information is in the same format as for the serving cell (ARFCN, RLA_P, PRIORITY_CLASS, C31). This information is not displayed if selecting using the C1/C2 procedure.

Orange : Information about the 2nd neighbour cell the MS is monitoring. This information is in the same format as for the serving cell (ARFCN, RLA_P, PRIORITY_CLASS, C31). This information is not displayed if selecting using the C1/C2 procedure.

Purple : Information about the 3rd neighbour cell the MS is monitoring. This information is in the same format as for the serving cell (ARFCN, RLA_P, PRIORITY_CLASS, C31). This information is not displayed if selecting using the C1/C2 procedure.

As noted in the parameter descriptions, many of these values will not appear if not selecting cells in the GPRS manner (i.e. clause 10 of GSM 05.08). Cells are only selected in the GPRS manner if PCCCH exists, or the network orders it in PACKET CELL CHANGE ORDER or PACKET MEASUREMENT ORDER messages [GSM 05.08:10.1]. Otherwise, C1/C2 (i.e. clause 6 of GSM 05.08) method will be used – See Test 1.1, 1.2, 1.3, 1.4, 1.5.

22. Field Test (ftd) – Group 7

Test 7.1, 7.2 – Information about Active PDP contexts

Available in: 7650

These tests display information about the MSes active PDP (Packet Data Protocol) contexts. A PDP context is a connection to an external network (such as an IP network). PDP traffic (i.e. IP packets) ride over the top of SNDCP, which rides over LLC, which in turns rides over the RLC/MAC layer. [GSM 03.60:5.6]

```
Field test
7.1
1. active PDP context

NSAPI/SAPI      5 3
Relia/Delay     3 4
Prece/peak      2 7
Mean/prior      B
VanJac/V.42bis
PDP addr of PDP context
10 208 103 243

Options          Exit
```

```

Field test
7.2
2. active PDP context

NSAPI/SAPI      0 0
Relia/Delay     0 0
Prece/peak      0 0
Mean/prior      3
VanJac/V.42bis  x x
PDP addr of PDP context
0 0 0 0

Options          Exit

```

```

Field test
7.1
1. active PDP context

NSAPI/SAPI      [Red] [Light Green]
Relia/Delay     [Dark Blue] [Light Green]
Prece/peak      [Light Green] [Light Green]
Mean/prior      [Light Green]
VanJac/V.42bis
PDP addr of PDP context
[Dark Blue]

Options          Exit

```

Red : The NSAPI (Network SAPI) used for the PDP context, in decimal. The SNDCP protocol uses the NSAPI to track and multiplex connections. The SAPI is a 4-bit value from 0-15. The meaning of the values are:

NSAPI	Meaning
0	Escape mechanism for future extensions
1	PTM-M (multicast) information
2-4	Reserved
5-15	Available for dynamically allocated user PDP connections

[3GPP TS 44.065:7.2]

Light Green : The SAPI used by the SNDCP for this NSAPI over the LLC protocol, in decimal. Whilst the NSAPI allows the SNDCP to multiplex several connections over a SAPI, the SAPI allows the LLC to multiplex several SNDCP connections over the radio interface. The SAPI is a 4-bit value from 0-15. The meaning of the values are:

SAPI	Service
1	GPRS Mobility Management messages – such as routing area updates, authentication, etc
2,8	Tunnelling of Messages
3,5,9,11	User data – SNDCP connections
7	SMS – some networks allow sending of SMS via the SGSN

[GSM 04.64:6.2.3]

More information about a particular SAPI can be found out in Tests 7.8 & Test 7.9.

Dark Blue : The reliability class of this PDP connection, in decimal. The reliability class is a 3-bit value which decides which layers of the protocol structure will be

operating in acknowledged/protected mode. Generally as the value increases, the reliability level decreases. The meaning of the values are:

Rel. Class	GTP Mode	LLC Mode	LLC protect	RLC Mode
1	ACK	ACK	Yes	ACK
2	NACK	ACK	Yes	ACK
3	NACK	NACK	Yes	ACK
4	NACK	NACK	Yes	NACK
5	NACK	NACK	No	NACK

This parameter can be negotiated. [GSM 03.60:15.2.3, GSM 04.08:10.5.6.5]

Yellow : The delay class of this PDP connection, in decimal. The delay class is a 3-bit value which is used by the network to decide how to manage the radio and other resources to affect the delay (latency) of the connection. The delay class is from 1-4, with 4 being the “best effort” (i.e. highest delay) and 1 having the smallest possible delay. This parameter can be negotiated. [GSM 03.60:15.2.2, GSM 04.08:10.5.6.5]

Pink : The precedence class of this PDP connection. The precedence class is a 3-bit value which is used by the network when accessing what data takes priority through a limited resource. The precedence class is from 1-3, with 1 being the highest priority and 3 being the lowest priority. For example, a PDP connection with precedence class of 2 will always have its QoS commitments honoured (or try to be honoured) over a PDP connection with precedence class 3. This parameter can be negotiated. [GSM 03.60:15.2.1, GSM 04.08:10.5.6.5]

Orange : The peak throughput class of this PDP connection, in decimal. The peak throughput class is a 4-bit value that specifies the expected maximum transfer rate of the connection. The network can limit the data transfer rate to this at any time if it wants, but it is also not a guarantee of the maximum transfer speed. The peak throughput value is from 1-9. The meaning of the values are:

Pk Throughput Class	Data rate (kbits)
1	8
2	16
3	32
4	64
5	128
6	256
7	512
8	1024
9	2048

This parameter can be negotiated. [GSM 03.60:15.2.4.1, GSM 04.08:10.5.6.5]

Purple : The mean throughput class of this PDP connection, in hexadecimal. The mean throughput class is a 5-bit value that specifies the average rate at which data is to be transferred over the connection lifetime. The network may limit the connection to this rate at any time. The mean throughput class is from 1-18, or 31. The meaning of the values are:

Mean Throughput Class	Data rate (bytes/hour) (bits/kbits)
1	100 (0.22bits)
2	200 (0.44bits)

3	500 (1.11bits)
4	1000 (2.2bits)
5	2000 (4.4bits)
6	5000 (11.1bits)
7	10000 (22bits)
8	20000 (44bits)
9	50000 (111bits)
10	100000 (0.22kbits)
11	200000 (0.44kbits)
12	500000 (1.1kbits)
13	1000000 (2.2kbits)
14	2000000 (4.4kbits)
15	5000000 (11.1kbits)
16	10000000 (22kbits)
17	20000000 (44kbits)
18	50000000 (111kbits)
31	Best effort (per need)

This parameter can be negotiated. [GSM 03.60:15.2.4.2, GSM 04.08:10.5.6.5]

Light Blue :

Dark Green :

Grey :

Red-Blue : The PDP address of this PDP context. The PDP address is a higher-level protocol specific address used for this connection. In the case of IPv4, this is specified as the 4 space-separated 8-bit numbers. [GSM 03.60:14.4, GSM 04.08:10.5.6.4]

Test 7.3 – RLC State Information

Available in: 7650

This test displays information about the Radio Link Control layer.

```

Field test
G 7.3
RLC state information
Downlink TS 2
Coding scheme 1
RLC mode down ACK
Uplink TS 2
Coding scheme 1
RLC mode up ACK
UL TBF OPEN
N3102 state 8
Options Exit

```

```

Field test
G 7.3
RLC state information
Downlink TS 0
Coding scheme 0
RLC mode down xxxx
Uplink TS 0
Coding scheme 0
RLC mode up xxxx
UL TBF xxxxx
N3102 state 8

Options Exit

```

```

Field test
G 7.3
RLC state information
Downlink TS ■
Coding scheme ■
RLC mode down ■
Uplink TS ■
Coding scheme ■
RLC mode up ■
UL TBF ■
N3102 state ■

Options Exit

```

Red : The current timeslot used for the downlink. (Since multiple slots can be used, I am not sure how this is displayed?) Can be 0-7.

Green : The current coding scheme used for the downlink. If 0, no TBF (Temporary Block Flow) exists on the downlink. Otherwise, the value can be from 1-4 which indicates the 4 GPRS coding schemes, CS-1 to CS-4 respectively. CS-1 to CS-4 define different levels of forward error correction (FEC), depending on radio conditions. CS-1 defines the highest level of FEC with the lowest data rate, and CS-4 defines the least level of FEC with the highest data rate. [GSM 05.03:5.1]

Dark Blue : The current RLC mode for the downlink, can be “ACK” or “NACK”, corresponding to acknowledged or not-acknowledged modes respectively. In acknowledged mode, the receiver acknowledges receipt of RLC blocks so the sender knows whether or not to send them again. “xxxx” is displayed if no TBF exists for the downlink. [GSM 04.60:9.3]

Yellow : The current timeslot used for the uplink. (Since multiple slots can be used, I am not sure how this is displayed?) Can be 0-7.

Pink : The current coding scheme used for the uplink. If 0, no TBF exists on the uplink. Otherwise, the value can be from 1-4 which indicates the 4 GPRS coding schemes, CS-1 to CS-4 respectively. [GSM 05.03:5.1]

Orange : The current RLC mode for the uplink, can be “ACK” or “NACK”, corresponding to acknowledged or not-acknowledged modes respectively. “xxxx” is displayed if no TBF exists for the downlink. [GSM 04.60:9.3]

Purple : Displays “OPEN” if a TBF exists on the uplink. Otherwise, “xxxxx” is displayed.

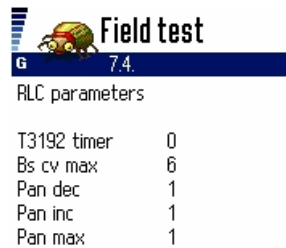
Light Blue : Value of the N3102 counter. This counter, if used (see Test 7.4) behaves a little like the Radio Link Timeout (See Test 01). This counter is decremented by the value PAN_DEC every time the RLC send window has reached its maximum (i.e. the difference between the last acknowledged packet sent and the last packet sent is at the maximum allowed value (WS)) for a certain period of time (T3182 – 5 seconds). When the counter reaches 0 (or less) the RLC layer will abort the TBF and attempt re-establishment. Conversely, for every time sent packets are acknowledged (by receipt

of PACKET UPLINK NACK/ACK message) this value is increased by the value PAN_INC (but never greater than PAN_MAX). Effectively, this behaves much like a control of maximum packet loss – if too much data is not acknowledged the counter causes the link to be aborted and re-attempted. On cell reselection the value is reset to PAN_MAX. This value also applies to unacknowledged RLC mode, since PACKET UPLINK NACK/ACK messages are still sent because they are used for channel quality analysis purposes. See Test 7.4 for further information. [GSM 04.60:9.3.2-3,13.3]

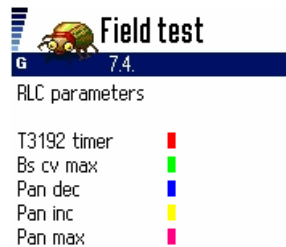
Test 7.4 - RLC parameters

Available in: 7650

This test displays information about the Radio Link Control layer.



Options Exit



Options Exit

Red : Initial value of the T3192 timer. This timer controls how long the MS will wait after the end of the TBF (i.e. after the final ACK) before releasing the resources. This timer is aborted if the network assigns additional downlink resources or changes those resources. It is a 3-bit value broadcast on BCCH (SI13) or PBCCH (PSI1/PSI13). It's meaning is interpreted as follows:

Value	Time
0	500ms
1	1000ms
2	1500ms
3	0ms
4	80ms
5	120ms

6	160ms
7	200ms

[GSM 04.60:12.24,13.1]

Green : Value of the BS_CV_MAX parameter, in decimal. This parameter is used in the calculation of the CV value which is sent in all uplink RLC data blocks to indicate to the network how many more RLC blocks are to be transferred. CV is calculated as (number of blocks remaining)/(number of timeslots in use). If CV is less or equal to BS_CV_MAX, it is left as is. Otherwise, it is set to 15 (maximum value – 0xF). Hence this value is the limit at which the real CV must fall below (or equal) before it is sent. BS_CV_MAX is a 4-bit value (in decimal) ranging from 0-15 broadcast on PBCCH (PSI1/PSI13) or BCCH(SI13). [GSM 04.60:9.3.1,12.24]

Blue : Value of the PAN_DEC parameter. This is a 3-bit value (in decimal) broadcast on the PBCCH (PSI1/PSI13) or BCCH (SI13) from 0-7. If this value is 0, the N3102 counter is disabled. See Test 7.3. [GSM 04.60:12.24]

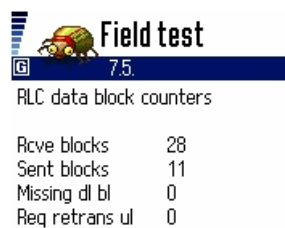
Yellow : Value of the PAN_INC parameter. This is a 3-bit value (in decimal) broadcast on the PBCCH (PSI1/PSI13) or BCCH (SI13) from 0-7. If this value is 0, the N3102 counter is disabled. See Test 7.3 [GSM 04.60:12.24]

Pink : Value used to calculate PAN_MAX parameter. This is a 3-bit value (in decimal) broadcast on the PBCCH (PSI1/PSI13) or BCCH (SI13) from 0-7. Let this value be 'x'. Then PAN_MAX is calculated by $4x+4$. Provided the N3102 is enabled, then the N3102 value in Test 7.3 should usually display this value ($4x+4$). See Test 7.3. [GSM 04.60:12.24]

Test 7.5 – RLC data block counters

Available in: 7650

This test displays statistics about the RLC blocks transferred during the current TBF (Temporary Block Flow).

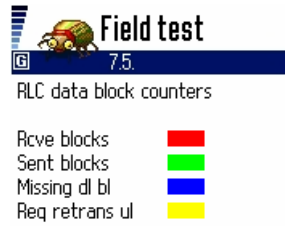


The screenshot shows a terminal window titled 'Field test' with a signal strength indicator on the left. Below the title bar, the test number '7.5' is displayed. The main content area shows the title 'RLC data block counters' followed by a list of statistics:

Rcve blocks	28
Sent blocks	11
Missing dl bl	0
Req retrans ul	0

Options

Exit



Red : The number of RLC data blocks received during the current TBF, in decimal.

Green : The number of RLC data blocks sent during the current TBF, in decimal.

Blue : The number of RLC data blocks (in acknowledged mode) that were not received, in decimal. [GSM 04.60:9.3]

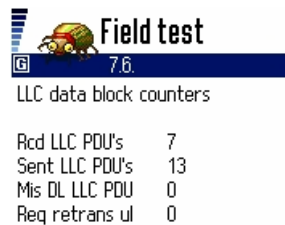
Yellow : The number of RLC data blocks (in acknowledged mode) that were not received by the network, and the network requested retransmission, in decimal. [GSM 04.60:9.3]

Most of the time these counters will be 0, since they are reset at the end of the TBF, which can be very short (perhaps only a few RLC/MAC data blocks).

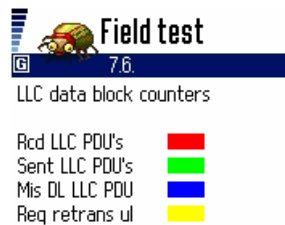
Test 7.6 – LLC data block counters

Available in: 7650

This test displays statistics about the LLC (Logical Link Control) data blocks transferred.



Options Exit



Options Exit

Red : The number of received LLC PDUs (Protocol Data Units) since initial GPRS-attach, in decimal.

Green : The number of sent LLC PDUs since initial GPRS-attach.

Blue : The number of LLC PDUs that were not correctly received. [GSM 04.64:8]

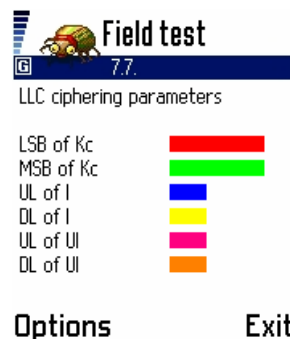
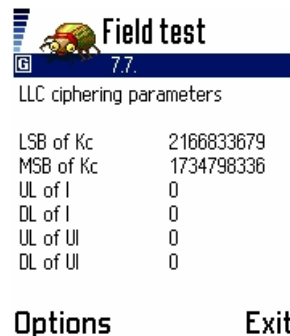
Yellow : The number of sent LLC PDUs that were not acknowledged and consequently resent. [GSM 04.64:8]

These counters do not appear to include data from the LLGMM SAPI (SAPI 1) (i.e. GPRS Mobility Management messages) and may likely only include User Data SAPIs. [GSM 04.64:6.2.3]

Test 7.7 – LLC ciphering information

Available in: 7650

This test displays information about the values used in the ciphering of LLC traffic. GPRS ciphering occurs at the LLC level, between the MS and the SGSN.



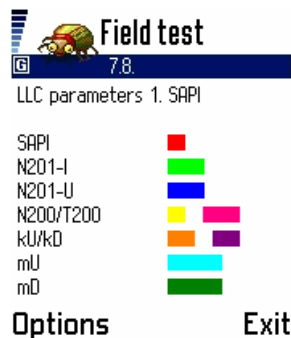
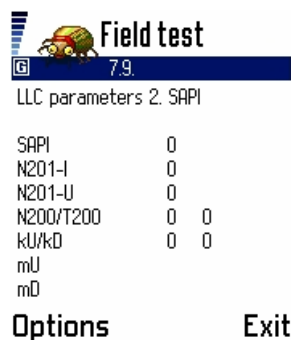
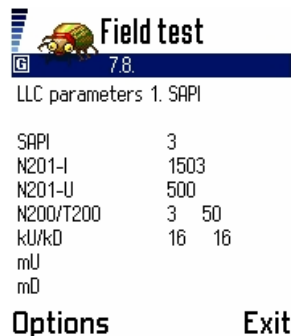
Red : The least significant 32-bits (i.e. bits 0-31) of the Kc, represented in decimal. The Kc is the 64-bit temporary key derived from the Ki and RAND parameter sent by the network used to cipher the GPRS traffic. The Kc and authentication works much the same way as it does for non-GPRS traffic, except it is over a higher level protocol. [GSM 03.60:6.8.1]

Green : The most significant 32-bits (i.e. bits 32-63) of the Kc, represented in decimal.

Test 7.8, 7.9 LLC parameters

Available in: 7650

These tests display negotiated parameters for the LLC protocol for up to 2 SAPs (Service Access Point). A SAP is a point of access to a higher level protocol, and this connection is identified by a SAPI (SAP Identifier). A SAPI is a bit like a port in the TCP protocol.



Red : Value of the SAPI used for this connection, in decimal. Current SAPIs are:

SAPI	Service
1	GPRS Mobility Management messages – such as routing area updates, authentication, etc
2,8	Tunnelling of Messages
3,5,9,11	User data – SNDCP connections
7	SMS – some networks allow sending of SMS via the SGSN

[GSM 04.64:6.2.3]

Light Green : N201-I value, in decimal. This value is the maximum number of octets that can be sent in the information field of an Information (i.e. acknowledged) LLC frame. This value has differing defaults for different SAPIs, and can also be

negotiated between the two LLC entities. N201-I can be from 140-1520 octets long. [GSM 04.64:8.9.5,8.9.9]

Dark Blue : N201-U value, in decimal. This value is the maximum number of octets that can be sent in the information field of an Unnumbered (i.e. unacknowledged) LLC frame. This value has differing defaults for different SAPIs, and can also be negotiated between the two LLC entities. N201-U can be from 140-1520 octets long. [GSM 04.64:8.9.5,8.9.9]

Yellow : N200 value, in decimal. The N200 value is generally used as the re-transmission attempt counter in the LLC protocol, for various Supervisory (S) and Acknowledged (I) frames. This value defaults to 3 for all SAPIs, and can be negotiated between the two LLC entities. N200 can be from 1-15 attempts. [GSM 04.64:8.9.4]

Pink : T200 value, in decimal. The T200 timer is generally used to decide how long the LLC entity will wait for some kind of response (i.e. acknowledgement or some other supervisory (S)) frame to be received. When this time period expires with no event the N200 counter may be checked. The default values for these timers vary for different SAPIs, and can be negotiated between the two LLC entities. T200 can be from 1 to 4095 deci-seconds (i.e. 0.1 to 409.5 seconds). [GSM 04.64:8.9.3]

Orange : Value of the kU parameter. The kU value is the window size for sent I (acknowledged frames), and is the maximum number of I-frames that can be unacknowledged at any time (before the sender (MS) stalls). The default value of the kU varies for different SAPIs, and can be negotiated between the two LLC entities. kU can be from 1-255 frames. [GSM 04.64:6.4.1.6,8.9.8]

Purple : Value of the kD parameter. The kD value is the window size for received I (acknowledged frames), and is the maximum number of I-frames that can be unacknowledged at any time (before the sender (Network) stalls). The default value of the kD varies for different SAPIs, and can be negotiated between the two LLC entities. kD can be from 1-255 frames. [GSM 04.64:6.4.1.6,8.9.8]

Light Blue : Value of the mU parameter. The mU value is the maximum buffer size in the MS for information (user) fields of I (acknowledged) frames that have been sent and are outstanding (i.e. not acknowledged). The default value of the mU varies for different SAPIs, and can be negotiated between the two LLC entities. Units are in 16-octets, from 9 to 24320 bytes. Sometimes this parameter is not displayed? [GSM 04.60:8.9.7]

Dark Green : Value of the mD parameter. The mD value is the maximum buffer size in the MS for information (user) fields of I (acknowledged) frames that have been sent and are outstanding (i.e. not acknowledged). The default value of the mD varies for different SAPIs, and can be negotiated between the two LLC entities. Units are in 16-octets, from 9 to 24320 bytes. Sometimes this parameter is not displayed? [GSM 04.60:8.9.7]

Test 7.10 – SNDCP data counters

Available in: 7650

This test displays statistics about the Sub-Network Dependent Convergence Protocol, the protocol used to carry the IP/X25/etc connection over the GPRS network. The SNDCP can multiplex multiple connections over a single SAPI. Each connection is identified by it's N-SAPI. [3GPP TS 44.065]

```

Field test
7.10.
SNDC data counters

Rcvd NPDUs      5
Sent NPDUs      12
Abort NPDU recep 0
Resent NPDUs    0

```

Options Exit

```

Field test
7.10.
SNDC data counters

Rcvd NPDUs      5
Sent NPDUs      12
Abort NPDU recep 0
Resent NPDUs    0

```

Options Exit

Red : The number of received N-PDUs (Network Protocol Data Units) by the MS, in decimal.

Green : The number of sent N-PDUs (Network Protocol Data Units) by the MS, in decimal.

Yellow : The number of N-PDUs that were received by the MS and aborted (due to duplication), in decimal.

Blue : The number of N-PDUs that were retransmitted by the MS, in decimal.

Appendix A – Typical Australian GSM network configurations

Disclaimer

These values are provided as a general idea into the configuration differences between the GSM networks. The information provided here is not guaranteed to be correct, and as mentioned can vary from region to region.

A.1 – Optus GSM

Country Code: 505
 Network Code: F02
 Bands: GSM900, GSM1800

General configuration

Please note these are the typical (most common) configurations used on this network throughout the country. Due to location specific requirements, actual configurations may vary in some areas.

Parameter	Location	Typical Value	Comment
MAX_RETRANS	BCCH/SI1	10b (4 attempts)	
CELL_BAR_ACCESS	BCCH/SI1	See below	
RE	BCCH/SI1	0b (No)	Call Re-establishment
EC	BCCH/SI1	1b (Yes)	Emergency calls
NCC Permitted	BCCH/SI2	0xFF	All NCCs
DTX	BCCH/SI3	01b (Must use)	DTX
RADIO-LINK_TIMEOUT	BCCH/SI3	0x4 (20)	
ATT	BCCH/SI3	1b (Yes)	IMSI (de)-attach required
BS-AG-BLKS-RES	BCCH/SI3		Access Grant/BCCH Ext exclusive blocks
CCCH-CONF	BCCH/SI3	See Note 1	
BS-PA-MFRMS	BCCH/SI3	11b (9 multiframe)	How often to listen to PCH
T3212	BCCH/SI3	80 (decihours)	Periodic Location Update timeout
CELL-RESELECT_HYSTERESIS	BCCH/SI3		
MS-TXPWR-MAX-CCH	BCCH/SI3		
ACS	BCCH/SI3,SI4	0b (find additional cell selection parameters in SI4, not SI7/8)	
NECI	BCCH/SI3	0b (No)	New establishment causes
RXLEV-ACCESS-MIN	BCCH/SI3	Varies, see below	
ECSC	BCCH/SI3	1b (Yes)	Early Classmark Sending Control
SI 2Ter	BCCH/SI3	1b (Yes)	SI 2Ter message sent
MULTIBAND_REPORTING	BCCH/SI2ter	Varies, see below	
CELL_BAR_QUALIFY	BCCH/SI4	See below	
CELL_RESELECT_OFFSET	BCCH/SI4	Varies, see below	
TEMPORARY_OFFSET	BCCH/SI4	000b (0dB)	
PENALTY_TIME	BCCH/SI4	Varies, see below	
POWER_OFFSET	BCCH/SI4		
SI13 Position	BCCH/SI4	0b (SI13 sent on BCCH Norm)	Where SI13 is sent (BCCH Norm or BCCH Ext)
PBCCH	BCCH/SI13	0b (No)	PBCCH used
SPGC_CCCH_SUP	BCCH/SI13	1b (Yes)	SPLIT_PG_CYCLE

			supported on CCCH in cell
PRIORITY_ACCESS_THR	BCCH/SI13		
NETWORK_CONTROL_ORDER	BCCH/SI13	00b (NC0)	How cell reselecting is decided (MS or network)/measurement reporting
NMO	BCCH/SI13	01b (NW2)	Network mode of operation
T3168	BCCH/SI13	001b (1sec)	
T3192	BCCH/SI13	000b (500msec)	
DRX_TIMER_MAX	BCCH/SI13	000b (0sec)	
ACCESS_BURST_TYPE	BCCH/SI13	1b (11bit)	
CONTROL_ACK_TYPE	BCCH/SI13	1b (RLC/MAC Control)	Default PACKET CONTROL ACKNOWLEDGEMENT message formatting
BS_CV_MAX	BCCH/SI13	0x6 (6)	
PAN_DEC	BCCH/SI13	001b (1)	
PAN_INC	BCCH/SI13	001b (1)	
PAN_MAX	BCCH/SI13	001b (8)	

Note 1: CCCH-CONF is usually 000b or 001b, which indicates BS_CC_CHANS=1 and BS_CCCH_SDCCH_COMB = FALSE (CCCH-CONF=000b) or TRUE (CCCH-CONF=001b).

In some cells, Optus will allocate a small CCCH and use the rest of timeslot 0 for SDCCH (including Cell Broadcast). In other cells, the full timeslot 0 will be used for the single CCCH.

Most base stations with GSM1800 equipment will be CCCH-CONF=000b (i.e. not combined).

Location Areas

The location areas are generally smaller closer to the CBD of a particular state or city, and generally increase in size as the distance from the CBD increases. The LAC (in decimal) is typically a 4 digit number, formatted by having the first digit indicate the state (i.e. 3 for Victoria, 2 for NSW, ...) and the next 3 digits indicate the Location Area. For the metropolitan areas, the second digit is typically 9.

Routing Areas

The routing areas are usually smaller than the location areas and independent of the location area boundaries. The RAI is typically a 3 digit number.

Cell Identities

The cell identities are unique for each cell (the GSM specifications do not require this, only within a LA must they be unique), and when expressed in decimal form a 5 digit number. The first digit specifies the state (i.e. 3 for Victoria, 2 for NSW), the next 3 digits indicate the actual cell number, and the last digit indicates the sector. 1-3 indicate a GSM900 cell, with 1-3 specifying the sector number, 7-9 indicate a GSM1800 cell with 7 being first sector, 8 being second sector, 9 being third sector.

I have seen the odd cell that does not conform to this numbering scheme – i.e. in Victoria I saw the cell ID “2513”.

Cell reselection parameters

These are fairly typical depending on type of site.

Standard GSM900 only metro site, or GSM900 selection parameters of combined GSM900/GSM1800

These also include sites at underground railway stations in Sydney and Melbourne (these are MULTIBAND_REPORTING=01b)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	000000b (0dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	00000b (0 second, since TEMPORARY_OFFSET=0)
2Ter	Varies, see below
MULTIBAND_REPORTING	00b or 01b

In GSM900 sites in proximity to GSM1800 sites, the 2Ter message is broadcast and MULTIBAND_REPORTING is set to 01b, which basically means (with Optus’s BA configuration) the MS has to report a GSM1800 cell (if available) in the first position of the measurement reports (in dedicated mode). The remaining positions must be filled with available GSM900 cells, and GSM1800 cells if no more GSM900 cells are found.

In GSM900 sites not in proximity to GSM1800 sites, the 2Ter message may or may not be broadcast. If it is broadcast, the MULTIBAND_REPORTING parameter is set to 00b, which means any position in the measurement reported can be filled with a cell from any band.

Metro site with GSM1800 (GSM1800 parameters)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	001010b (20dB)
TEMPORARY_OFFSET	000b (0dB)

PENALTY_TIME	11111b (0 seconds, subtract CELL_RESELECT_OFFSET)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	11b

GSM1800 sites have MULTIBAND_REPORTING set to 11b, meaning the first three positions of the measurement report must be filled with GSM900 cells (if available), and the remaining 3 positions for reporting GSM1800 cells. If no more GSM1800 cells are found, GSM900 cells must be reported.

GSM1800 cells typically have a negative CELL_RESELECT_OFFSET to discourage all MSes from camping on them.

GSM900 Microcell in high density area (CBD, inner city, busy intersection)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	001010b (20dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	11111b (0 seconds, subtract CELL_RESELECT_OFFSET)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	01b

The microcells typically have a negative CELL_RESELECT_OFFSET to discourage all MSes from camping on them.

As mentioned before, although most sites conform to these settings, there can be exceptions.

Cell Barring

The Optus network rarely ever uses cell barring, even for sites under development. The network sets CELL_BAR_QUALIFY=0 and CELL_BAR_ACCESS=0 which indicates a cell of “Normal” priority (to Phase 2 MS) and a non-barred cell (to Phase 1 MS)

Cell broadcast

The network broadcasts on the CBCH pages with Message Identifier 050 (0x0032) on most sites. The text in the message contains the name of the suburb which has the intended majority of the site’s coverage, or nearby landmarks.

GPRS configuration

The Optus GPRS configuration is a fairly simple one – the CCCH/BCCH are used (not the PCCCH/PBCCH). The network operates in mode II, meaning no paging coordination or combined LA/RA updates. Network Control Order is 0, combined with no PCCCH mean the standard GSM (C2) procedure is used for cell reselection.

The network does not support sending of SMS over the GPRS radio interface (i.e. via SGSN).

The network supports GPRS coding schemes CS1-CS4, and dynamic uplink assignment is used.

Spectrum

Type	ARFCN range	Frequency Range (MS Rx) MHz	Freq Range (MS Tx) MHz
GSM900	43-83	943.6-951.8	898.6-906.8
GSM1800	573-599		
GSM1800	673-737		

GSM1800 is now extensively used in capital city CBDs and inner-metropolitan areas. In Melbourne and Sydney, it is also extensively used in the suburbs.

GSM900 base stations typically use odd ARFCNs for their C0 (i.e. BCCH carriers).

Other

Feature	Comment
Ciphering	A5/1 always
GPRS Ciphering	GEA1 always
EFR	Supported
FR	Supported
Data	Supported, to 9.6kbps
GSM SS	

A.2 – Telstra GSM

Country Code: 505
 Network Code: F01
 Bands: GSM900, GSM1800

General configuration

Please note these are the typical (most common) configurations used on this network throughout the country. Due to location specific requirements, actual configurations may vary in some areas.

Parameter	Location	Typical Value	Comment
MAX_RETRANS	BCCH/SI1	10b (4 attempts)	
CELL_BAR_ACCESS	BCCH/SI1	0b	See below
RE	BCCH/SI1	0b (No)	Call Re-establishment

EC	BCCH/SI1	1b (Yes)	Emergency calls
NCC Permitted	BCCH/SI2	0xFF	All NCCs
DTX	BCCH/SI3	01b (Must use)	DTX
RADIO-LINK_TIMEOUT	BCCH/SI3	0x4 (20)	
ATT	BCCH/SI3	1b (Yes)	IMSI Attach
BS-AG-BLKS-RES	BCCH/SI3		Access Grant/BCCH Ext exclusive blocks
CCCH-CONF	BCCH/SI3	000b	1 CCCH, not combined with SDCCH
BS-PA-MFRMS	BCCH/SI3	010b (4 multiframe)	How often to listen to PCH
T3212	BCCH/SI3	30 (decihours)	Periodic Location Update timeout
CELL-RESELECT_HYSTERESIS	BCCH/SI3		Hysteresis for inter-LA cell reselection
MS-TXPWR-MAX-CCH	BCCH/SI3		
ACS	BCCH/SI3,SI4	0b (find additional cell selection parameters in SI4, not SI7/8)	
NECI	BCCH/SI3	0b (No)	New establishment clauses
RXLEV-ACCESS-MIN	BCCH/SI3		
ECSC	BCCH/SI3	1b (Yes)	Early Classmark Sending Control
SI 2Ter	BCCH/SI3	Varies, see below	SI 2Ter message sent
MULTIBAND_REPORTING	BCCH/SI2ter	Varies, see below	SI 2ter not sent in all cells
CELL_BAR_QUALIFY	BCCH/SI4	Varies, see below	See below
CELL_RESELECT_OFFSET	BCCH/SI4	Varies, see below	
TEMPORARY_OFFSET	BCCH/SI4	000b (0dB)	
PENALTY_TIME	BCCH/SI4	Varies, see below	
POWER_OFFSET	BCCH/SI4		
SI13 Position	BCCH/SI4		Where SI13 is sent (BCCH Norm or BCCH Ext)
PBCCH	BCCH/SI13		PBCCH used
SPGC_CCCH_SUP	BCCH/SI13		SPLIT_PG_CYCLE supported on CCCH in cell
PRIORITY_ACCESS_THR	BCCH/SI13		

NETWORK_CONTROL_ORDER	BCCH/SI13		How cell reselecting is decided (MS or network)/measurement reporting
NMO	BCCH/SI13		Network mode of operation
T3168	BCCH/SI13		
T3192	BCCH/SI13		
DRX_TIMER_MAX	BCCH/SI13		
ACCESS_BURST_TYPE	BCCH/SI13		8bit or 11bit
CONTROL_ACK_TYPE	BCCH/SI13		
BS_CV_MAX	BCCH/SI13		
PAN_DEC	BCCH/SI13		
PAN_INC	BCCH/SI13		
PAN_MAX	BCCH/SI13		

Cell reselection parameters

These are fairly typical depending on type of site.

Standard GSM900 only, or GSM900 parameters on GSM900/1800 site

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	000000b (0dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	00000b (0 second, since TEMPORARY_OFFSET=0)
2Ter	Varies, see below
MULTIBAND_REPORTING	00b, or 10b, or (00b on BCCH, 10b on SACCH)

In GSM900 sites in proximity to GSM1800 sites, the 2Ter message is broadcast and MULTIBAND_REPORTING is set to 10b*, which basically means (with Telstra's BA configuration) the MS has to report a GSM1800 cell (if available) in the first two positions of the measurement reports (in dedicated mode). The remaining positions must then be filled with cells of the band of the current cell, and if there are still positions left over, they shall be filled with the strongest cells of any band.

*or the BCCH MULTIBAND_REPORTING parameter is set to 00b, and the SACCH MULTIBAND_REPORTING parameter is set to 10b.

GSM1800 parameters on GSM900/1800 site

The GSM1800 band is not usually included in the idle mode BA list, so an MS will rarely encounter such a GSM1800 BCCH. The network does not allow camping or establishing a connection on most GSM1800 sites. There are some, however, that are an exception to this rule (see 'Cell barring' below).

GSM900 Microcell in high density area (CBD, inner city, busy intersection)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	001010b (20dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	11111b (0 seconds, subtract CELL_RESELECT_OFFSET)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	On BCCH: 00b or 10b On SACCH: 10b

The microcells are penalised with a cell reselect offset of -20dB, in a similar strategy to Optus. They set MULTIBAND_REPORTING (on the SACCH) to 10b.

In building or special coverage cell

In-building cells are common around places like the Melbourne CBD, and are usually on the GSM900 band.

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	Varies, see below
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	00000b (0 second, since TEMPORARY_OFFSET=0)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	00b or 10b (SACCH)

The inbuilding cells often have a positive CELL_RESELECT_OFFSET to encourage mobile stations in the building to camp on them, instead of straying to metro-cells from outside.

Cell barring

As mentioned above, many GSM1800 sites are 'locked out' completely for camping by normal MS. It appears IMSI attach / location update are not possible on these sites.

Other GSM1800 sites are 'visible' as neighbouring GSM900 cells include them in the BA list (by means of SI 2Ter), however they are marked as having priority barred. These cells can still be camped on temporarily after a connection has been cleared (as allowed by the GSM specifications) and using Test 19 in Net Monitor. Connections can be established from these sites.

Cell broadcast

The network broadcasts on the CBCH pages with Message Identifier 050 (0x0032) on most sites. The text in the message contains the name of the suburb which has the intended majority of the site's coverage, or nearby landmarks.

A.3 – Vodafone GSM

Country Code: 505

Network Code: F03

Bands: GSM900, GSM1800

General configuration

Please note these are the typical (most common) configurations used on this network throughout the country. Due to location specific requirements, actual configurations may vary in some areas.

Parameter	Location	Typical Value	Comment
MAX_RETRANS	BCCH/SI1	10b (4 attempts)	
CELL_BAR_ACCESS	BCCH/SI1	0b	See below
RE	BCCH/SI1	0b (No)	Call Re-establishment
EC	BCCH/SI1	1b (Yes)	Emergency calls
NCC Permitted	BCCH/SI2	0xFF	All NCCs
DTX	BCCH/SI3	01b (Must use)	DTX
RADIO-LINK_TIMEOUT	BCCH/SI3	0x4 (20)	
ATT	BCCH/SI3	1b (Yes)	IMSI Attach
BS-AG-BLKS-RES	BCCH/SI3		Access Grant/BCCH Ext exclusive blocks
CCCH-CONF	BCCH/SI3	000b	1 CCCH, not combined with SDCCH
BS-PA-MFRMS	BCCH/SI3	100b (6 multiframe)	How often to listen to PCH
T3212	BCCH/SI3	20 (decihours)	Periodic Location Update timeout
CELL-RESELECT_HYSTERESIS	BCCH/SI3		Hysteresis for inter-LA cell reselection
MS-TXPWR-MAX-CCH	BCCH/SI3		
ACS	BCCH/SI3,SI4	0b (find additional cell selection parameters in SI4, not SI7/8)	
NECI	BCCH/SI3	0b (No)	New establishment clauses
RXLEV-ACCESS-MIN	BCCH/SI3	Varies, see	

		below	
ECSC	BCCH/SI3	1b (Yes)	Early Classmark Sending Control
SI 2Ter	BCCH/SI3	Varies, see below	SI 2Ter message sent
MULTIBAND_REPORTING	BCCH/SI2ter	Varies, see below	SI 2ter not sent in all cells
CELL_BAR_QUALIFY	BCCH/SI4	0b	See below
CELL_RESELECT_OFFSET	BCCH/SI4	Varies, see below	
TEMPORARY_OFFSET	BCCH/SI4	Varies, see below	
PENALTY_TIME	BCCH/SI4	Varies, see below	
POWER_OFFSET	BCCH/SI4		
SI13 Position	BCCH/SI4	0b (SI13 sent on BCCH Norm)	Where SI13 is sent (BCCH Norm or BCCH Ext)
PBCCH	BCCH/SI13	0b (No)	PBCCH used
SPGC_CCCH_SUP	BCCH/SI13	0b (No)	SPLIT_PG_CYCLE supported on CCCH in cell
PRIORITY_ACCESS_THR	BCCH/SI13		
NETWORK_CONTROL_ORDER	BCCH/SI13	00b (NC0)	How cell reselecting is decided (MS or network)/measurement reporting
NMO	BCCH/SI13	01b (NW2)	Network mode of operation
T3168	BCCH/SI13	000b (500msec)	
T3192	BCCH/SI13	111b (200msec)	
DRX_TIMER_MAX	BCCH/SI13	111b (64sec)	
ACCESS_BURST_TYPE	BCCH/SI13	0b (8-bit)	8bit or 11bit
CONTROL_ACK_TYPE	BCCH/SI13	0b (4 access bursts)	Default PACKET CONTROL ACKNOWLEDGEMENT message formatting
BS_CV_MAX	BCCH/SI13	0x4 (4)	
PAN_DEC	BCCH/SI13	001b (1)	
PAN_INC	BCCH/SI13	010b (2)	
PAN_MAX	BCCH/SI13	100b (20)	

Location Areas

Location area codes are typically based on a postcode of a nearby town or suburb. In some lower density areas, the LAC could be the postcode of a suburb some distance away (since network efficiency takes precedence).

Cell Identities

The cell identities are unique for each cell (the GSM specifications do not require this, only within a LA must they be unique), and when expressed in decimal form a 5 digit number. The first digit specifies the state (i.e. 3 for Victoria, 2 for NSW), the next 3 digits indicate the actual cell number, and the last digit indicates the sector. 1-3 indicate a GSM900 cell, with 1-3 specifying the sector number, 7-9 indicate a GSM1800 cell with 7 being first sector, 8 being second sector, 9 being third sector.

Microcells do not follow this convention, and typically have 4 digit IDs, of the form 8xx0, where 'xx' is the cell number.

Cell reselection parameters

These are fairly typical depending on type of site.

Standard GSM900 only metro site, or GSM900 selection parameters of combined GSM900/GSM1800

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	000000b (0dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	00000b (0 second, since TEMPORARY_OFFSET=0)
2Ter	Varies, see below
MULTIBAND_REPORTING	00b or 01b

In GSM900 sites in proximity to GSM1800 sites, the 2Ter message is broadcast and MULTIBAND_REPORTING is set to 01b, which basically means (with Vodafone's BA configuration) the MS has to report a GSM1800 cell (if available) in the first position of the measurement reports (in dedicated mode). The remaining positions must be filled with available GSM900 cells, and GSM1800 cells if no more GSM900 cells are found.

In GSM900 sites not in proximity to GSM1800 sites, the 2Ter message may or may not be broadcast. If it is broadcast, the MULTIBAND_REPORTING parameter is set to 00b, which means any position in the measurement reported can be filled with a cell from any band.

CBD metro site with GSM1800 (GSM1800 parameters)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	

CELL_RESELECT_OFFSET	010100b (40dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	00000b (0 second, since TEMPORARY_OFFSET=0)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	01b

The CBD GSM1800 metrocells have a 40dB positive cell reselect offset, to highly encourage camping. Combined with a higher RXLEV-ACCESS-MIN, this results in a much higher C2 value.

Inner city metro site with GSM1800 (GSM1800 parameters)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	000000b (0dB)
TEMPORARY_OFFSET	000b (0dB)
PENALTY_TIME	00000b (0 second, since TEMPORARY_OFFSET=0)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	01b

GSM900 Microcell in high density area (CBD, inner city, busy intersection)

Parameter	Value
RXLEV-ACCESS-MIN	
MS-TXPWR-MAX-CCH	
CELL_RESELECT_OFFSET	001010b (20dB)
TEMPORARY_OFFSET	100b (40dB)
PENALTY_TIME	00000b (20 seconds, since TEMPORARY_OFFSET != 0)
2Ter	1b (broadcast)
MULTIBAND_REPORTING	01b

The microcells have a temporary offset applied for 20 seconds to discourage idle mode camping by phones moving through (in vehicles). However, pedestrian phones will receive a 20dB boost (to encourage camping).

As mentioned before, although most sites conform to these settings, there can be exceptions.

Cell broadcast

The network broadcasts on the CBCH pages with Message Identifier 050 (0x0032) on most sites. The text in the message contains the name of the suburb which has the intended majority of the site's coverage, or nearby landmarks.

Cell Barring

A number of sites have been noted with CELL_BAR_ACCESS=1b and CELL_BAR_QUALIFY=0b (meaning bar for both Phase 1 & 2). These sites all seem to have their C0 (i.e. BCCH carrier) on ARFCN=85. If an MS is forced to camp on these sites, all CHANNEL REQUEST messages on the RACH appear to be ignored (no IMMEDIATE ASSIGNMENT [EXTENDED/REJECT] are sent back by the BTS). No cell broadcasts appear on these cells.