

Bluetooth GPRS Connectivity, with Nokia 6230i on MTN.

Alan Robert Clark

May 11, 2007

I have a Fedora Core 3 setup, using a Gigabyte Technology USB Bluetooth Dongle, GN-BTD02, and a Nokia 6230i on the MTN network.

Packages required were:

```
gnome-bluetooth-0.5.1-5.FC3.1.i386.rpm
libbtctl-0.4.1-3.i386.rpm
openobex-1.0.1-1.i386.rpm
bluez-bluefw-1.0.6
bluez-hcidump-1.11-1
bluez-libs-2.10-2
bluez-utils-2.10-2
```

all of which are yum-able.

module

Plug in USB module, and `/var/log/messages` says:

```
kernel: usb 4-1: new full speed USB device using uhci_hcd and address 2
kernel: usb 4-1: device not accepting address 2, error -71
kernel: usb 4-1: new full speed USB device using uhci_hcd and address 3
kernel: Bluetooth: HCI USB driver ver 2.8
hcid[3852]: HCI dev 0 registered
kernel: usbcore: registered new driver hci_usb
hcid[3852]: HCI dev 0 up
hcid[3852]: Starting security manager 0
```

hciconfig

Running `hciconfig` reveals:

```
hci0:  Type: USB
      BD Address: 00:14:85:92:BD:0F ACL MTU: 192:8  SCO MTU: 64:8
      UP RUNNING PSCAN ISCAN
      RX bytes:101 acl:0 sco:0 events:13 errors:0
      TX bytes:300 acl:0 sco:0 commands:13 errors:0
```

which is the dongle.

hcidtool

Running `hcidtool scan` gives:

Scanning ...

```
00:15:2A:27:D0:BD      Nokia 6230i
```

which is the BD address of my particular phone.

Using the BD address to interrogate it further reveals: (`hcitool info 00:15:2A:27:D0:BD`)

Requesting information ...

```
BD Address: 00:15:2A:27:D0:BD
Device Name: Nokia 6230i
LMP Version: 1.1 (0x1) LMP Subversion: 0x382
Manufacturer: Cambridge Silicon Radio (10)
Features: 0xbf 0xee 0xf 0x00 0x00 0x00 0x00 0x00
          <3-slot packets> <5-slot packets> <encryption> <slot offset>
          <timing accuracy> <role switch> <sniff mode> <RSSI>
          <channel quality> <SCO link> <HV3 packets> <u-law log>
          <A-law log> <CVSD> <paging scheme> <power control>
          <transparent SCO>
```

Other useful commands (in the form of `hcitool command 00:15:2A:27:D0:BD`) are `rss`, `lq`, `tp` to show received signal strength, link quality, and transmit power level.

sdptool

Next to interrogate the services offered by the phone, we want Dial-up Networking (DUN), so issue `sdptool search --bdaddr 00:15:2A:27:D0:BD DUN` which produces:

```
Searching for DUN on 00:15:2A:27:D0:BD ...
```

```
Service Name: Dial-up networking
```

```
Service RecHandle: 0x100a5
```

```
Service Class ID List:
```

```
"Dialup Networking" (0x1103)
```

```
"Generic Networking" (0x1201)
```

```
Protocol Descriptor List:
```

```
"L2CAP" (0x0100)
```

```
"RFCOMM" (0x0003)
```

```
Channel: 1
```

```
Language Base Attr List:
```

```
code_IS0639: 0x656e
```

```
encoding: 0x6a
```

```
base_offset: 0x100
```

```
Profile Descriptor List:
```

```
"Dialup Networking" (0x1103)
```

```
Version: 0x0100
```

Look for the channel number, which in this case is 1, the default assumed by `rfcomm`, but it isn't always 1.

rfcomm

`rfcomm` connects the remote DUN service, via a Bluetooth tunnel, to a device on the linux box.

The command `rfcomm connect 0 00:15:2A:27:D0:BD 1` reveals:

```
Connected /dev/rfcomm0 to 00:15:2A:27:D0:BD on channel 1
```

```
Press CTRL-C for hangup
```

0 for `/dev/rfcomm0` and 1 for channel 1, which can be left out in my case.

This is after a (rather quick) dual PIN request on the phone and on the screen. This is where trouble was had last time around. Use 1234 on both, and the “pairing” occurs. On the phone, configure (for that computer) to “Auto-connect without confirmation”.

NOTE: You CANNOT use the same dongle on two different machines without deleting the “pairing” on the Cell. Confuses the daylights out of EVERYTHING.

Once this has been done, you can *bind* the channel to the socket.

`rfcomm bind 0 00:15:2A:27:D0:BD 1` will “bind” the device to the channel on demand.

PPP

Now to set up a ppp connection over the usb over the bluetooth!!

OK. Much, Much, Much frustration later.....

Turns out that the Nokia 6230i is a little buggy. Even under 'Doze, I get the same brick wall, either “Subscribe to GPRS first”, or “GPRS Access Point invalid”. We have swapped SIM's, phones, etc, and, yup, its the phone.

The problem is in the ppp and call setup order. Traditionally, ppp is started, calls chat to do call setup. wvdial replaced chat, and has a chat mode, which works for all my other dial-ups, but not this one. wvdial prefers to be started first, and fires up ppp when it needs to. This mode works.

So, in `/etc/wvdial.conf`, we have:

```
[rfcomm0]
Modem = /dev/rfcomm0
Baud = 921600
SetVolume = 0
Dial Command = ATDT
Init1 = ATZ
FlowControl = CRTSCTS

[Dialer AlanMTN]
Username = clark
Password = hi
Phone = *99#
Stupid Mode = 1
Init1 = ATZ
Init2 = AT+CGDCONT=1,"IP","internet"
Inherits = rfcomm0
```

then the command `wvdial AlanMTN` connects beautifully:

```
--> WvDial: Internet dialer version 1.54.0
--> Initializing modem.
--> Sending: ATZ
ATZ
OK
--> Sending: AT+CGDCONT=1,"IP","internet"
AT+CGDCONT=1,"IP","internet"
OK
--> Modem initialized.
--> Sending: ATDT*99#
--> Waiting for carrier.
ATDT*99#
CONNECT
```

```

~[7f]}#0!;} } }2}#}$@#}!}$}%\}"&} }*} } g}%~
--> Carrier detected. Starting PPP immediately.
--> Starting pppd at Thu Aug 17 23:22:01 2006
--> pid of pppd: 14718
--> Using interface ppp0
--> pppd: dem
--> pppd: dem
--> pppd: dem
--> local IP address 172.26.7.228
--> pppd: dem
--> remote IP address 10.6.6.6
--> pppd: dem
--> primary DNS address 10.204.32.245
--> pppd: dem
--> secondary DNS address 209.212.96.1
--> pppd: dem
Caught signal #2! Attempting to exit gracefully...
--> Terminating on signal 15.
--> pppd: dem
--> pppd: dem
--> Connect time 23.7 minutes.
--> pppd: dem
--> pppd: dem
--> Connect time 23.7 minutes.
--> pppd: dem
--> pppd: dem
--> Disconnecting at Thu Aug 17 23:45:44 2006

```

As can be seen, a simple Ctrl-C (SIGINT, or 2) closes the connection gracefully.

While the ppp connection is running,

```
/sbin/route
```

shows the routing table that is set up, and

```
/usr/sbin/pppstats
```

keeps tabs on traffic. This agrees with the numbers found under Call Register — GPRS data counter — Data sent in last session.

Solved mail problem. Put the nameservers in MTN order (/etc/resolv.conf):

```

nameserver 10.204.32.245
nameserver 209.212.96.1
nameserver 146.141.16.134

```

and set up the SMTP server as mail.mtn.co.za. (For Vodacom users, its smtp.vodacom.co.za). All works perfectly.

IPTables and NAT routing.

Lot of reading material here!!! At the end of the day, I have a simple little script gprs to fire up the whole thing:

```

rfcomm bind 0 00:15:2A:27:D0:BD
echo 1 > /proc/sys/net/ipv4/ip_forward

```

```
/sbin/iptables -A POSTROUTING -t nat -o ppp0 -j MASQUERADE
```

```
/sbin/iptables -A INPUT -j DROP -m state --state NEW,INVALID -i ppp0
/sbin/iptables -A FORWARD -j DROP -m state --state NEW,INVALID -i ppp0
```

```
wvdial --config ./wvdial.conf AlanMTN
```

```
/sbin/iptables --flush
/sbin/iptables --table nat --flush
```

Remember that wvdial waits until a Ctrl-C to drop the connection, and the firewall is then reset. The firewall presents the entire home subnet with a single (masqueraded) connection to the internet, from MTN's perspective, I only have one machine at home :-)

MTN Charging model at 30 Aug 2006:

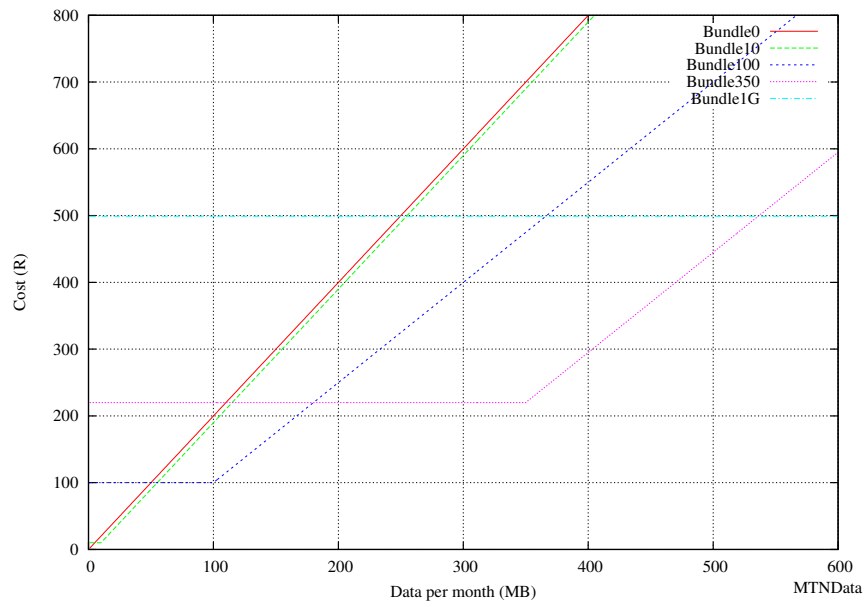


Figure 1: MTN Data “packages”

Note the gap between 350MB and 1GB packages. According to MTNBroadbandDude, they're testing the waters in that gap.

Package	0	10	100	350	1024
Cost	0	10	100	220	499
InLimitRate		1	1	0.63	0.49
OutOfBundle	2	2	1.5	1.5	1.25

Rollover day for my 100MB package is the 26th of the month. October was the first full month.

Month	Tx. Bytes	Rx. Bytes
Oct	13 467 714	69 606 767
Nov	24 060 227	173 609 120
Dec	23 480 177	177 604 000
Feb	20 183 045	124 647 259
Mar	32 880 086	141 051 222
Apr	23 377 211	101 166 806

Stand-alone SIM for Internet

Got a brand new SIM card on a “ProData” package for the spare Nokia 6230i that will serve as the “Fixed-mobile” (What a name :-) internet access at home. Since the phone has never been fiddled with, herewith then the procedure for setting everything up from scratch!

1. Put new SIM in, switched on phone. Did not seem to require a PIN.
2. Goto—Bluetooth Menu—Bluetooth On. Phone’s name changed to ”Internet”.
3. `hcitool scan` reveals the new BD number to be 00:15:2A:27:F9:A0
4. `rfcomm release rfcomm0` to unbind the other phone.
5. `rfcomm connect 0 00:15:2A:27:F9:A0 1`
6. set pins (1234) on both phone and screen dialogues. Then hangup with \hat{C} .
7. edit the gprs script above to issue the Bind to this BD number (00:15:2A:27:F9:A0)
8. Goto—Bluetooth Menu—Paired Devices—NeedleNardleNoo (Options)— Auto-conn. without confirmation set to yes
9. hit `./gprs` and it all just works!
10. Menu—Call Register—GPRS Data Counter. Leave it on that screen and plug it in!!!!

Images

Do not do the `rfcomm connect` bit, but do do Applications/System Tools/Bluetooth File Sharing from the Bluez stack.

On the phone, collect the pic from the gallery, Options/Send/via Bluetooth on an individual basis, unfortunately. Have set up camera to do full 1280x1024 shots, since I won’t use it often, and might as well have decent pics :-)

Hit the Delete All button on the phone! (Kills the screensaver. too :-(No way to get it back to the phone!!))

(Move to the MMC card from the gallery.)