Using SMS on

WRT54G3G Wireless-G Router

for 3G/UMTS Broadband

(Models WRT54G3G-EU/UK/AU and all WRT54G3GV2)

Version 1.0

November 1, 2007

1 Scope

This document describes the use of SMS features for the WRT54G3G-UK, -EU, -AU and all models of the WRT54G3GV2.

2 Description

There are two types of SMS features, SMS messaging and SMS commands.

2.1 SMS messaging

This feature allows the user to send and receive SMS messages through the Router's Graphical User Interface (GUI, also known as the web-based utility). For example, the user can check the credit balance of the user account.

The user can activate up to five trusted SMS message senders as an option in the GUI.

To open the SMS messaging window, click the **SMS** button on the *Applications & Gaming → SMS* screen.

Incoming SMS messages will be displayed in this window.

The user can also compose and send messages via this window.

The phone number format can be either format, a long format with complete country code or a short code. Example: +44778712456 or 121.

Messages will be stored up to the SIM card capacity (received and sent). Older messages will not automatically be deleted even when the Router is rebooted. The SIM card will not receive new incoming messages when messages have exceeded SIM card capacity. The user has the option to delete messages manually or automatically. The default is manual deletion. In the automatic deletion mode, the Router deletes the oldest messages first so that the number of SIM messages will be limited. The setting is configurable, and the default number of saved SIM messages is eight.

Delete the SMS-INT and SMS-*(SMS commands) messages immediately after they have been read.

2.2 SMS commands

This feature allows an Authorized User (AU), such as an IT manager, to command the Mobile Broadband Router (MBR) to perform any of the following actions:

1. Reboot
2. Connect to a mobile network
3. Send a Wake-On-LAN (WOL) packet to a device on the LAN

4. Send a WOL packet to all devices on the LAN

The Router is preconfigured by the GUI to enable these features (default is disabled) and to include the list of trusted phone numbers from which SMS commands will be sent (up to five numbers).

For added security, the following command sequences should be executed.

1. An SMS is sent by the AU to the Router to initiate the command sequence
2. The Router sends back an SMS with a key, which is a random string of seven bytes.
3. Then the AU sends an SMS with the command encrypted with the string using RC4.

The SMS Command list is provided in the table below:

Command	Description
SMS-INT	INITIATE: Start the SMS command sequence.
SMS-RBT	REBOOT: Reboot the MBR through SMS The command should be enabled on the admin page.
SMS-CNT	CONNECT: Restart the 3G connection.
SMS-WOL	Send the WOL packet to one device. The device will be identified by the MAC address or by the alias name as predefined in the GUI. Enable the WOL command on the admin page. 1) Enter the MAC address in the first row of the admin page. 2) Then send the SMS-INT. 3) Then send either: SMS-WOL 00:01:02:03:04:05 ## same MAC address or SMS-WOL PC1## PC1 alias to MAC in admin page

Command	Description
SMS-WOLALL	Send WOL commands to all devices; no argument will follow the command word. The command should be enabled on the admin page.
SMS-RECNT (Optional)	Terminate the 3G connection and connect again (this is actually what the SMS-CNT command will perform). If connected already, the command will disconnect and then reconnect. If disconnected, the command will initiate connection.
SMS-STATUS (Optional)	Reply to the AU with Firmware Version, Online Status, Connection Time, Connection Type (UMTS/GPRS), Signal Status, IMSI, WAN-IP, MAC Address.
SMS-RESET (Optional)	Data card reset: This only works if the Router is disconnected from the 3G network.

The MBR monitors all incoming SMS messages. Upon receiving an SMS-INT message, the MBR will start to initiate the SMS command sequence and set the X1 timer to five minutes (configurable).

1. An AU starts the sequence by sending the SMS-INT.

2. The MBR checks to see if the message was sent from a trusted phone number.

3. The MBR send back a message to the originating phone number containing a key (random string of 7 bytes).

4. The AU will use the RC4 algorithm and the key to encrypt the SMS commands and send them back to the MBR.

5. Upon receiving the command and authenticating it successfully, the MBR will execute the command and send back an acknowledge message via SMS.

6. If the correct command is not received within five minutes (configurable timer, X1), the MBR will abort the sequence.
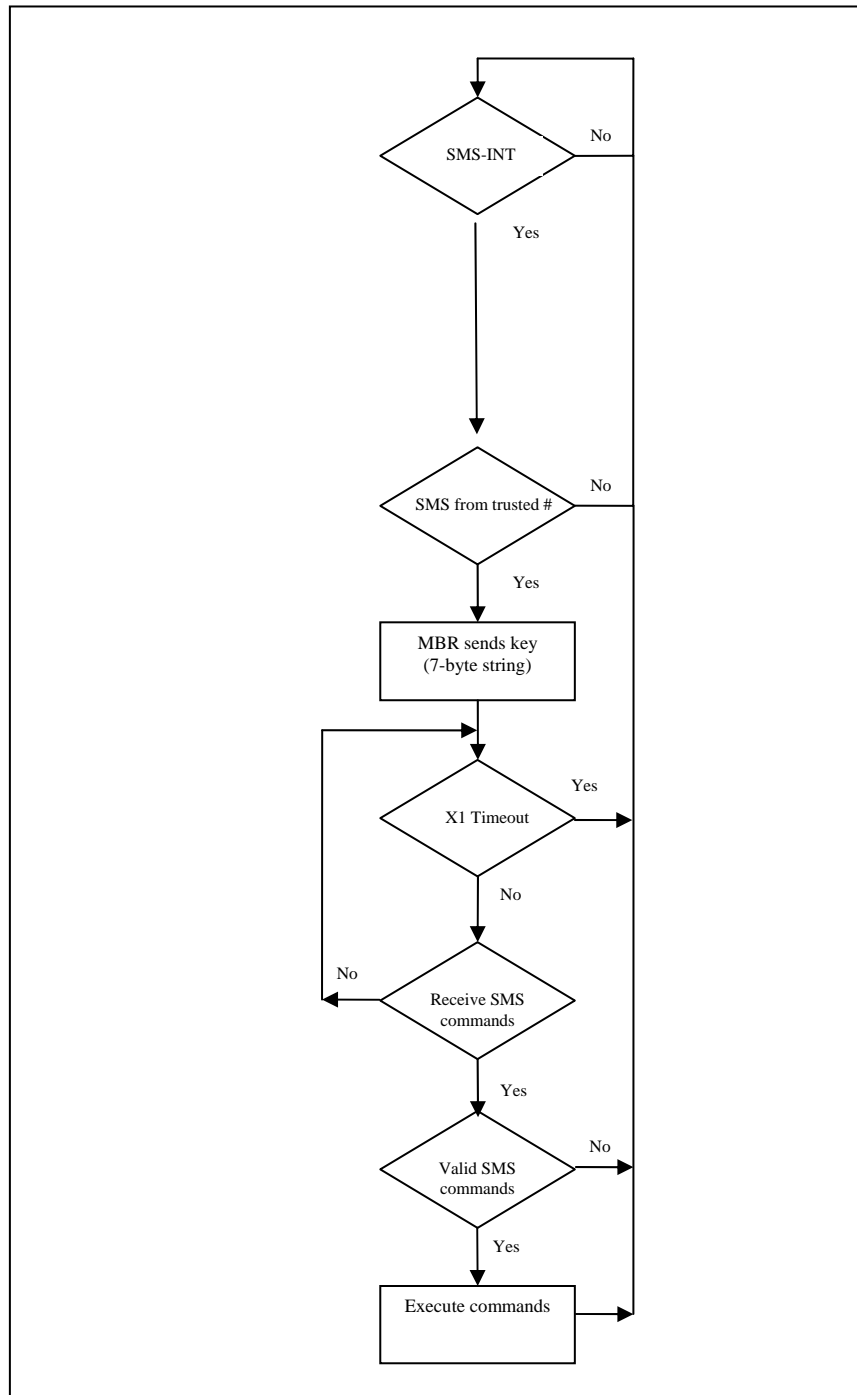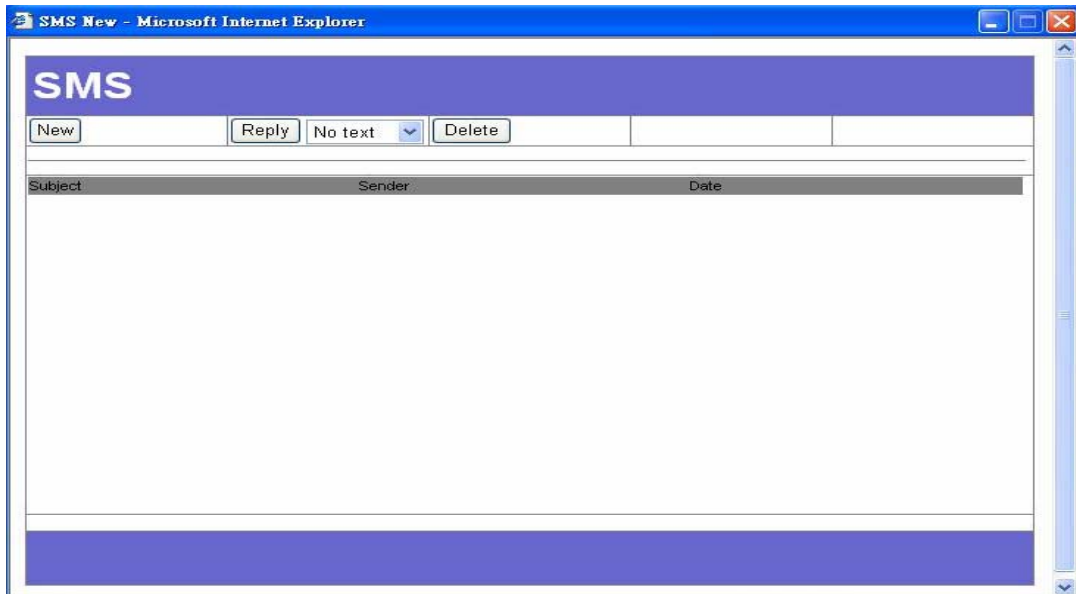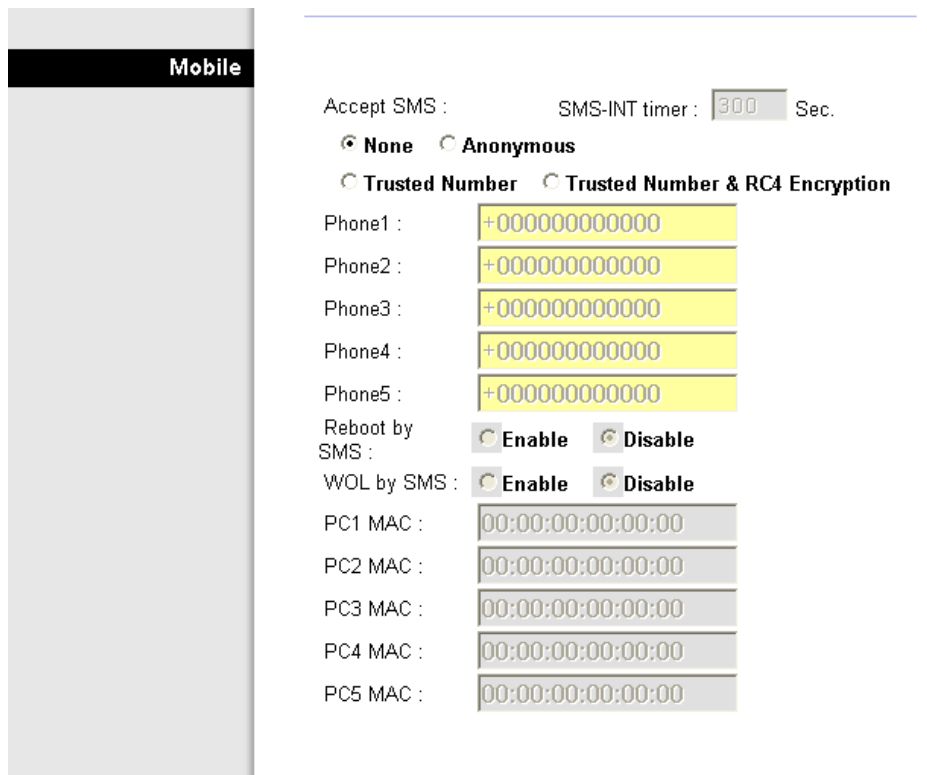
Figure 1: Flow chart for SMS commands

Figure 2: SMS message window

Figure 3: SMS commands and trusted numbers

2.3 RC4 encryption

Here are the steps to start RC4 encryption in either Linux or Windows with the Crypt::RC$ module installed.

1) On the Router's *Administration* → *Management* screen, enable the following:

    a) Accept RC4 SMS
    b) Reboot by SMS
    c) Authentication by Phone number + enter your own number

2) Send an SMS with this body text: **SMS-INT**

3) Wait for a reply using the key. Example: 9cf81d8.

4) Using the returned key, use the Perl program to encrypt the command SMS-CNT :

    sms_encode.pl SMS-CNT 9cf81d8

and receive:

    dc96cbf1888eb3

5) Send your encrypted command in the body of an SMS to the Router:

    dc96cbf1888eb3

6) Wait a few moments for the command to be executed.

Here is an example script: "sms_encode.pl"

```perl
#!/usr/bin/perl

use Crypt::RC4;
use bytes();

if($#ARGV lt 1 ) {
        die "Usage $0 command key\n";
}
$encrypted = RC4( $ARGV[1], $ARGV[0] );

for( $i=0;$i < length($encrypted);$i++) {
        printf("%02x",ord substr($encrypted,$i,1));
}
```

```
printf("\n");

#$decrypt = RC4( $passphrase, $encrypted );
```