APPLIED SATELLITE ENGINEERING-MACHINE-TO-MACHINE

This resource is brought to you by ASE M2M.

We provide the following for satellite machine-to-machine applications.

- *Hardware—Modems to fully operational terminals.*
- *Antenna and Cabling Solutions.*
- *Data Plans and Monitoring.*
- *Server Applications.*
- *Tracking—Position tracking and Data tracking including alerts.*
- *Remote Control of Assets.*
- *Development—Hardware, Software, Firmware, Enclosures, Full Solutions.*
- *Prototyping.*
- *Full Manufacturing.*
- *Certifications, Iridium, CE, FCC, IEC, and others.*

Contact information.

Contact us at anytime to discuss your particular application and needs.

- *Email: info@ase-corp.com*
- *Phone +1.480.443.1424 (Americas)*
- *Phone +353 85 7615506 (EMEA)*
- *http://m2m.ase-corp.com*

Hughes 9502

System Integrators Guide

Version 1.5
May 2012

inmarsat.com/

Contents

Introduction

1.1 Purpose of this guide

This Hughes 9502 System Integrators Guide is intended for System Integrators (SIs) and Solution Providers.

The guide describes the installation and set-up of the Hughes 9502 BGAN M2M terminal and the creation of internet connections to user equipment. It covers configuration of the terminal and of the user equipment to establish effective power management of the remote equipment and security management for the system. Terminal firmware upgrade is also covered.

1.2 Scope

This document provides an overview of BGAN M2M and detailed instructions on how the terminal configuration command sets are used to manage the terminal.

This document contains some specific details of the Hughes 9502 terminal, its command sets and its installation but more details may be found in the manufacturer's user guides.

1.3 Reference documents

The following documents are referenced in this Integrator's Guide and are considered essential material for the Integrator:

1. Hughes 9502 Fixed Satellite Terminal User Guide. Document No. 3004146.
2. Hughes AT Command Reference (Provided as HTML document with each release)
3. Hughes 9502 SMS Remote Control Feature User Guide Revision (Available from Hughes on application and will require an NDA))

The reader should refer to the latest version of these Reference Documents as maintained on the Inmarsat website.

1.4 Terminology

The Hughes 9502 terminal is designed to deliver Inmarsat BGAN M2M services. This document is specifically directed at integrators for the Hughes 9502 terminal. The terms Hughes 9502 terminal and BGAN M2M terminal are used interchangeably throughout this document.

1.5 Hughes 9502 Terminal Firmware Version

This version 1.4 of the Integrators Guide is applicable to the terminal firmware version 5.9.1.3.

2 BGAN M2M Overview

BGAN M2M is a new service offering to the existing portfolio of BGAN services that will allow users to connect to remote devices and applications at low data rates. It is based entirely on the current BGAN network and infrastructure and there are no changes to the Inmarsat provisioning process. This means that BGAN M2M will benefit from proven, reliable technology.

BGAN M2M uses a subset of BGAN features:

- Only standard (background) IP connections are supported;
- Streaming connections are not supported
- Voice, ISDN and fax are not supported
- SMS is supported. This is used as one mechanism for remote machine-to-machine configuration and it may also be used to send regular text messages if needed

2.1 Remote operation

The Hughes 9502 is a fixed product using the BGAN M2M service. The remote nature of the installation will require the System Integrator to focus on a number of BGAN M2M capabilities:

- How to use the power saving modes of the terminal
- Remote configuration of the terminal
- Automatic recovery
- Connecting user equipment through a range of SCADA interfaces

The number of user devices (SCADA device or application) that can be managed by a terminal is determined by the method of IP addressing employed by the manufacturer. The Hughes 9502 terminal uses direct IP addressing (Basic NAT) and so uses a PDP context for each addressable device. The maximum number of contexts supported by the Hughes 9502 terminal is ten. Note, however, that the Watchdog and Always On features only support one user currently.

2.2 Commercial opportunities

Potential market and application areas are seen as:

Utilities	Deployment into Smart Grid including support for SCADA protocols
Oil & Gas	Wellhead, pump and pipeline monitoring applications including SCADA support
Retail Banking	Remote ATM and point of sale solutions
Environmental	Weather monitoring, water level management

The application or solutions used within these markets can be easily re-purposed to other market opportunities including mining, aid and civil government.

3 User Terminals

The only BGAN M2M user terminal available as of March 2012 is the fixed BGAN 9502 terminal.

Out of the box the BGAN M2M 9502 comprises:

- Indoor Unit (IDU)
- Outdoor Unit (ODU)
- A 10m RF cable and adapter to connect the two units

Accessories

- Optional mounting brackets are available for the IDU and ODU

Integrators will also require USB device drivers if they intend to connect a computer to the USB port of the IDU to configure it. The USB port is for configuration only and is designed for use when the Ethernet interface is already connected to user equipment.

The ODU is a passive flat panel antenna that will require pointing to establish RF communication with the BGAN network. It also provides GPS signals for the GPS receiver that is integral to the IDU.

The IDU provides all of the functions of the terminal including the provision of IP connectivity via the BGAN satellite network. A detailed description of the Hughes 9502 terminal is contained in the Hughes 9502 Fixed Satellite Terminal User Guide. This section contains a brief overview of some key features.

The front and back panels of the IDU are shown below in Figure 1.

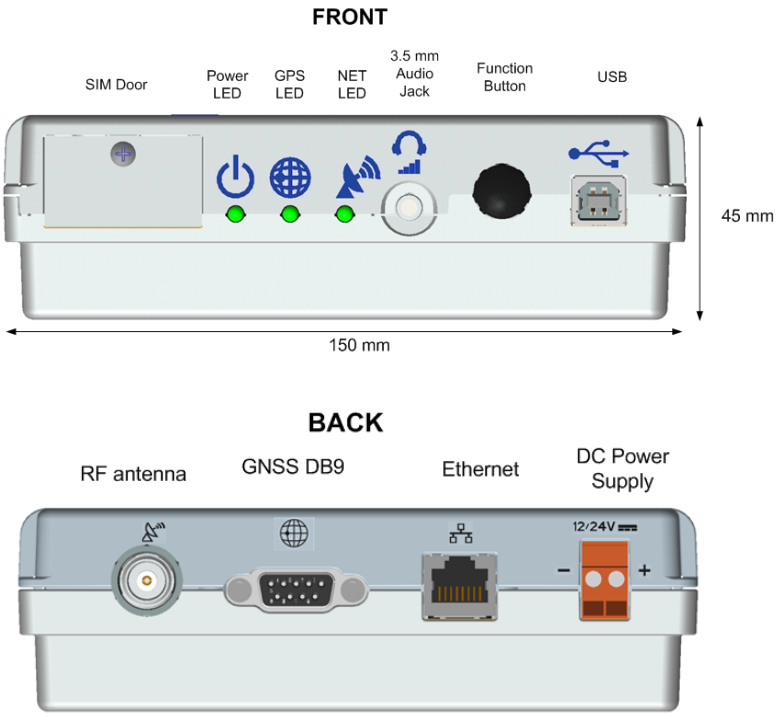


Figure 1: BGAN M2M 9502 Indoor Unit

The terminal interfaces are as follows:

- The DC Power Supply supports nominal 12V and 24V. As soon as power is connected the terminal will power up. When power is disconnected the terminal will power down.
- The RJ45 Ethernet connection is used to connect all user equipment. The Ethernet connection can also be used for configuration and control of the terminal such as via the WebUI.
- The DB9 RS232 serial interface can accept NMEA 0183 data from an external GNSS device e.g. from a GLONASS receiver. (See notes below on GNSS and NMEA for more information). It cannot be used for other serial data. Maintaining a nominal voltage of 12V between Pins 5 (ground) and 9 (positive) of this port will power the terminal down until the

voltage is removed (see sections on GPIO). (The applied voltage can be between 2.5V DC to 50V DC, but12V is recommended).

Note that the implementation of GNSS interfaces can vary. The GNSS feature on the Hughes 9502 requires that it receives one of the following NMEA sentences in order to get a fix: RMC or GGA.

- The RF connector is for connection to the ODU using the supplied RF cable only, which must not be modified.
- The USB connector is to enable the connection of a computer to configure the terminal. Note that this is its only purpose. PDP contexts cannot be activated for the USB port.
- The audio jack provides an audio tone or voltage level to assist in antenna pointing. Steady voltage levels allow a voltmeter to be used during pointing. The pointing signal quality of 50dB is about 2.9V DC and each dB is about 0.15V DC, so expected voltages are approximately 2.5 to 3.2V DC. See the table under notes below for actual voltages measured during testing. This signal is always provided in installation mode and does not need to be configured to be on. A voltmeter cannot be used directly touching the jack; you must have a 3.5 mm stereo plug inserted and then touch the wires from the plug. (The tip and ring contacts of the plug are for the positive voltmeter probe, and the sleeve contact is for the negative voltmeter probe).

Notes on GNSS

A Global Navigation Satellite System (GNSS) is a system of satellites that provide autonomous geo-spatial position-fixing with global coverage. Currently, there are two satellite constellations: the US GPS system and the Russian GLONASS system. A number of other countries are developing additional systems e.g. the Chinese Beidou system and the European Galileo system. A number of augmentation systems that enhance the basic GPS/GLONASS systems are also available.

Notes on NMEA

The NMEA 0183 standard describes a serial ASCII protocol used in the marine industry for communication between instruments. Messages are referred to as sentences. The Hughes 9502 accepts a subset of the sentences defined by NMEA. Consult the Hughes 9502 Fixed Satellite Terminal User Guide RD.1 for more information.

Notes on Pointing Signal voltages

The following voltages were measured on the audio jack whilst pointing during testing (MMI is the indicated signal strength on the 9502's WebUI):

MMI	VM (DC)
41	1.66
45	2.25
46	2.38-2.40
47	2.51-2.60
49	2.81-2.96
50	2.96
51	3.09-3.10

BGAN M2M Service Features

4 Key Features of BGAN M2M

This section describes how BGAN M2M uses the more general BGAN features and it identifies key capabilities of the BGAN M2M.

4.1 PDP context

Up to eleven PDP contexts (primary or secondary) may be simultaneously established on the BGAN M2M terminal although one PDP context is reserved for performing remote activities e.g. firmware upgrade, remote configuration and remote debugging. PDP contexts can be configured to be automatically established at power-on. The Hughes web user interface (WebUI) is used to configure the terminal. LaunchPad is not supported.

A secondary context is effectively a private channel within a primary PDP context used for a specific user application. You can only set up a secondary context if a primary context exists and it will be encapsulated in the same packet flow using the same IP address.

4.2 Dynamic host configuration protocol (DHCP)

The 9502 terminal has a DHCP server that can allocate IP addresses to devices connected locally using dynamic or static assignment of IP addresses from a configurable address range. Each IP device connection will establish its own PDP context. The terminal's default local IP address is 192.168.128.100. This address is configurable if needed. Reference the Hughes 9502 Fixed Satellite Terminal User Guide for more information (see RD.1).

4.3 Network modes

The BGAN M2M terminals can operate in basic NAT mode or Relay mode. NAT mode does not impact the number of contexts/connected equipment that can be supported, but Relay Mode supports only one PDP context/connected device.

In NAT mode, the terminal assigns the local device an IP address from the configured DHCP range of addresses and the terminal will translate between the global IP address and the local IP address. Note that this Basic NAT in the 9502 does not modify IP port numbers so port forwarding or port translation is not required.

In Relay mode, the terminal's DHCP server will initially assign the local device an IP address from the configured DHCP range of addresses. Once the PDP context is established, the global IP address will be pushed to the local device at the next DHCP renewal request. At this point in time, the basic NAT is turned off in the terminal and all traffic is passed directly to the local device. Note that during set-up and tear-down of Relay mode contexts, there will be an IP connectivity delay between the local device and the terminal/network because the local device's DHCP lease must expire and get renewed before proper IP connectivity can resume.

4.4 Access point name (APN)

APN's will be provisioned as per existing BGAN services.

The following need to be considered when provisioning a BGAN M2M user:

- Typically an APN with a dynamically-assigned IP is used when using Hughes 9502 terminal features (although use of a static global IP address is possible):
    - Remote access to the WebUI
    - Remote configuration

- Remote log upload
- Remote firmware upgrade

NOTE: There is a default APN for firmware upgrade (the 9502 terminal is hard-coded with a default-free pro-rated APN)

- By default, the following APN “update.bgan.inmarsat.com”, which is used for firmware upgrading, is required to be provisioned to the subscriber by the DP. This will allow free over-the-air firmware upgrades. As a result, there will be only nine (9) of the usual ten (10) APNs available for provisioning in the HLR. This default APN allows unbilled access to official firmware upgrade files.
- DPs should be aware that subscribers do not have to be provisioned with all available APNs as the terminal will be deployed in a fixed location. There will be instances of terminal location where a specific APN must be used to comply with commercial or national agreements, referred to as ‘forced routing’.

4.5 SIM cards

BGAN M2M SIM cards will only work in BGAN M2M terminals, and a BGAN M2M terminal will only accept a BGAN M2M SIM. When provisioning a BGAN M2M SIM card, there will only be the options for BGAN M2M price packages.

Note the following when programming a BGAN M2M SIM:

- SIMs should not have SIM PIN enabled since the UT is assumed to be unattended in typical applications. The terminal will not function unattended if a SIM PIN is enabled. For SIM security please refer to the terminal user guide on personalisation. It is possible to lock the SIM to the terminal for security
- Inmarsat recommends the SIM be programmed with an MSISDN because this is required for remote SMS control and will be shown on the main page of the 9502 WebUI. However, this is not required for the service to work and some operators may not want the installer to know the number for security reasons.

4.6 Terminal features

The integrator will only connect user equipment through the Ethernet connection on the terminal. Other ports on the terminal are dedicated to other uses.

The terminal has an integrated GPS module to establish the terminal position. It also has the ability to accept GNSS position data through a dedicated serial port and if this signal is provided by the integrator, the terminal will use the most recently provided source of position.

The terminal can be configured in a number of ways:

- The terminal has a USB port that is dedicated to local configuration of the terminal and this can accept commands from the manufacturer’s web interface using a PC or MAC computer. You must have the USB device driver installed on the computer to use the USB port (refer to the Hughes or Inmarsat web pages for them)
- The terminal can also be configured locally using the same web interface connected through Ethernet port or remotely
- It is also possible to locally configure the terminal using AT commands via Ethernet or USB connections or remotely using SMS-encoded commands

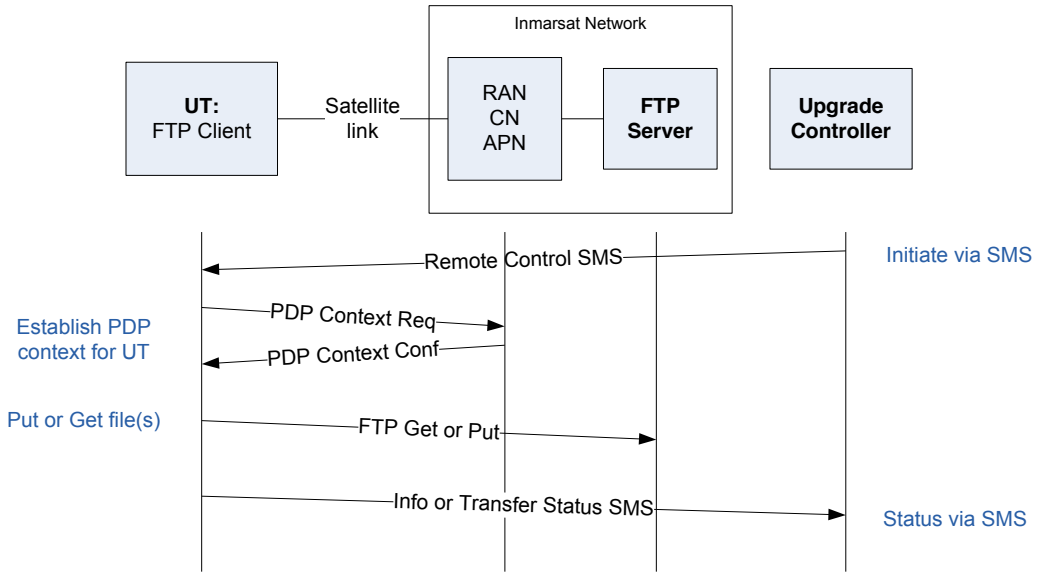
More information on configuring the terminal is provided in sections 5-8

4.7 Terminal firmware upgrade

This section covers remote upgrade of the terminal. It is also possible to upgrade the terminal locally.

4.7.1 Remote terminal firmware upgrade

The terminal firmware will be upgraded remotely using an FTP client installed on the terminal. The process flow for upgrade is shown below.



The remote upgrade procedure can be a one step or two step process:

1. The UT is commanded to download the new software binary ("firmware"). There are two options: one for an automated upgrade once the firmware has been downloaded and a second option for deferred upgrade. The download process uses the *IGETFW* command - see the Hughes 9502 SMS Remote Control Feature (RD.3) and the terminal gets a binary file from a specified FTP server. The default (all fields left blank) uses Inmarsat hosted servers. The 9502 will self-manage flash storage space in which the new file will be downloaded.

   When using the free firmware upgrade service, the server is located in a "walled garden" and protects the UT from access to and from the Internet.

   Once the UT completes the IGETFW command it sends an SMS or AT command to indicate success or failure.

2. If the delayed option of the *IGETFW* command was used you will then use the *IUPDFW* command to upgrade the terminal firmware:

   - You must know the file name that you downloaded as part of the *IGETFW* command to use the *IUPDFW* command properly (See RD3 for more details)
   - The UT uses a flag file in flash to indicate it is doing an upgrade and stores any information it will require on restart, such as the SMS return number

   On restart, if the UT finds an upgrade file, it determines its state and sends an SMS or unsolicited AT command to indicate the outcome of the upgrade. The UT boot code includes enhancements to recover from the download of a bad binary and switch back to the old release.

4.7.2 Local terminal firmware upgrade

Firmware upgrades may also be implemented locally using a dedicated Hughes Upgrader application. The application and supporting files will be made available to the user for download onto a PC or MAC which is connected to the terminal using an Ethernet or USB cable. User instructions are provided below:

Note: When using Vista or Windows 7 operating systems, you must run the upgrader application as the Administrator. Right click on the Upgrader executable and select “Run as Administrator”.

The basic method is as follows:

1. Install the application and supporting files onto the configuration computer
2. Connect the computer to the modem with an Ethernet cable and power up the modem. The order is not important and it is not necessary to connect the antenna or have a SIM installed.
3. Start up the Hughes application and select the firmware upgrade and/or the PIC upgrade (see Figure 2 below for the PC upgrader example). Other configuration options should be ignored
4. Select the ‘Upgrade’ button. The application will display progress until the modem is reset and the application declares the operation has successfully upgraded the terminal. Note that it may be necessary to unblock the firewall during the terminal upgrade by accepting this option in response to a warning window

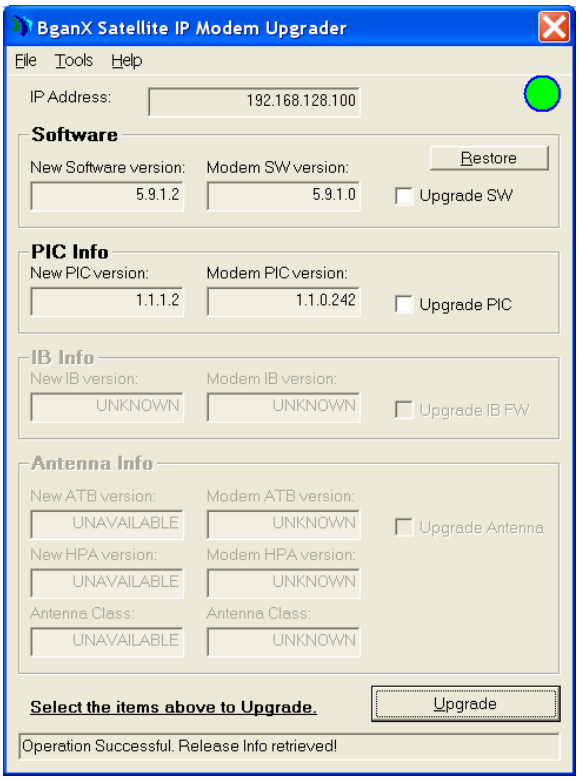


Figure 2: Local Firmware Upgrade Application

4.8 Third party interference detection: L-band spectrum scanning

The M2M terminal includes an L-band scanning mode to detect third party sources of external interference. The terminal can be commanded into scanning mode by the WebUI, AT command or SMS command. Refer to the Hughes 9502 User Manual (RD.1) for information on how to configure this feature.

The terminal does not reboot to go into scanning mode but during the scan, the terminal will be offline to the BGAN network. It will automatically reboot to return to normal operation once the scan is complete. In scanning mode the terminal checks the 41MHz of L-band spectrum (1518 to 1559MHz). The terminal will take autonomous action to invoke resiliency circuitry within itself if an interference signature is detected and will issue a scan report to this effect, either on the AT port or in an SMS depending on how the scan was initiated. The scan should take no longer than one minute.

If the terminal installer expects that interference may be an issue, it is possible to invoke the resilience circuitry through WebUI configuration.

If interference is suspected during normal operations then an SMS can be sent to the terminal to activate the scan or to manually invoke the resilience circuitry. However, note that the interference could impact reception of these commands.

For more detail see the Hughes 9502 Fixed Satellite Terminal User Guide (RD.1).

4.9 Watchdog

The BGAN M2M terminal includes a watchdog mechanism that can be used to periodically verify the UT network connectivity and take action if a problem is detected.

Watchdog pings are used to detect connectivity and as they are bits of data just like any other user data they require an active PDP context in order to be transmitted.

The ping mechanism will also act as a keep alive on the PDP context to prevent it from being torn down. The ping mechanism has the following configuration parameters:

- Watchdog Enable/Disable (Default off)
- 3 Ping IP address (1 Required, no default)
- Number of pings passes to attempt before declaring a problem (default 3)
- Watchdog/Heartbeat Frequency in minutes (default 8 hours). Minimum time is 5 minutes
- Ping required: if not set, then the system will not try pinging on timer expiration if user data was transmitted within the watchdog period. Timeouts

When the terminal is powered up and registered with the network, it is put into the Regional Beam.

Once a PDP context is established, it goes into the Narrow Beam; 200 kHz bandwidth is allocated at whatever frequency the GRM allocates. The PDP context effectively sets up a mapping between the SGSN and GGSN in the RAN to say that the UT exists and this mapping is maintained for 12 hours. The 12 hours is defined in the APN and is the default setting although it is configurable.

While in the Narrow beam, there is a 90s timeout if no data is sent and the UT is put back into regional beam (but the PDP context is maintained for 12 hours)

The ping acts as a keep-alive: several points to note here:

- If ping required is set to Yes, it will ping at the configured interval even if data is already being sent
- If ping required is set to No, no pings will be sent if data has been sent within the configured interval

Note that when you change watchdog/ping information and “apply settings” a terminal reboot is required.

4.10 Wake on LAN (any packet)

Wake on LAN is a hardware feature that allows the UT to be put into a special low power mode where almost all the electronics are turned off. The LAN port of the terminal will generate 10BaseT link pulses of 200ns duration every 16ms whilst the Wake on LAN power saving mode is active so that all connected Ethernet devices remain alive. This means that user equipment is able to send packets of data at any point which will cause the UT to power on and receive the data. The power consumed in Wake on LAN mode will be less than 10mW when operating at 12V.

Note that whilst in the Wake on LAN mode the UT is not registered on the network and so it is not possible to command the UT by SMS or communicate with it in any way.

The UT includes a configurable idle timer to control when the UT shuts down into the Wake on LAN mode. The UT will declare the link idle if no packets are received on the Ethernet port within the idle time. Additionally, the UT can be set up to power down at a configurable time of day.

For the idle timer to work properly the user equipment must not send periodic packets. For example, periodic ARPs and DHCP lease renewals must be suppressed. This may require the device to have a static IP address.

Problems could also arise with packets being sent from an external source in the Internet causing the idle timer to be reset. If the UT has a public IP address then packets may be sent to it from the Internet (e.g. hackers). If the user equipment responds to any packet then this will reset the idle timer.

The user equipment must handle the fact that when Wake on LAN is active and traffic resumes, the UT will take in the order of a minute to power up, register, attach and establish an active PDP context. To accommodate this, the user equipment could retransmit data packets if it does not receive a response. See ‘Wake on Any Packet Setup Procedure’ in section 9 for more information.

4.11 Wake on general purpose input output (GPIO)

The UT can also be powered off via a GPIO control line on the DB9 GNSS serial port. If a voltage is applied to Pin 9 of the serial port with pin 5 as Ground, the UT will power down. It will power up when the voltage is removed. The voltage can be 2.5V DC to 50V DC and the recommended value is 12V DC.

Note that whilst the UT is being maintained in a powered off state by GPIO it is not possible to command the terminal by SMS.

4.12 Security

The following security features are supported by the terminal:

- Ethernet MAC filtering
- UT administration password. (This is the same password that may be set to control access to the WebUI)
- SMS control password
- White list for SMS control. (This is a list of subscriber numbers that have been authorised to send the UT configuration commands)
- AT command password lock
- SIM personalisation

- Phone-to-SIM
- DP SIM lock
- SP SIM lock

4.13 Interfacing to SCADA

A primary implementation for BGAN M2M will be to provide a connection between a remote terminal unit (RTU) and a SCADA collection server at the user's data centre. SCADA has a number of message formats but in essence they are all data when viewed from the BGAN M2M perspective.

Generally there are many protocols that may be used in M2M applications but they should all work over IP and Inmarsat has tested many of the standard protocols. Note that the application may need to be modified or configured to operate correctly over the M2M IP link.

A number of SCADA RTUs will output serial data and the integrator will be required to encapsulate these data streams into TCP/IP to be routed to the collection server. Many serial-to-IP adapters exist and several have been tested by Inmarsat.

Intelligent Device (ID):

These will be devices that can control the UT directly using the AT command set, but giving minimal information back to the serial interface i.e. Connect, Dial, No dial tone. They will also be able to establish the PDP context independently from the "Auto activate on Data" option in the 9502 interface.

Non Intelligent Device (NID):

These devices will have no control of the UT and are only a mechanism of transmitting the collected data to a central server.

Configuration

The Hughes 9502 UT has a number of ways it can be configured. It can be configured locally or remotely across the BGAN network. Locally, there are a number of physical interfaces that can be used.

There are three methods that can be used to configure the terminal:

- Using the built in web server called Web UI
- Using modem AT commands
- Using SMS commands (remotely)

This section describes these various options.

The solution provider will develop a methodology for using the various configuration methods depending on the circumstances.

There are two main use cases to be covered:

- Installation
- Operational use

Generally, local configuration of a deployed terminal will be useful only during installation because typically the terminal will not be in a manned location. After installation is complete, the remote form of commanding is necessary to configure the terminal.

Another consideration is the number of similar installations required. It may be efficient for a solution provider to develop a terminal configuration on a local unit and to upload this configuration to a fileserver so that it can be downloaded to a number of terminals in the field. Remote configuration file update is covered in the Use Case section of this document.

5 Local and Remote Control

There are a number of message channels that can be used to connect the terminal with its configuring equipment.

- Using the Ethernet connection on the UT (Local)
- Using the USB connection on the UT (Local)
- Using the BGAN network (Remote)

The Ethernet connection may be used to:

- Connect a PC to access the WebUI to configure the terminal
- Connect a third party equipment that communicates using AT commands, which could be user equipment e.g. intelligent SCADA RTUs

The USB port may only be used to connect a PC to access the WebUI to configure the terminal

The BGAN network may be used to support remote terminal management both using SMS exchanges and using WebUI. AT messages can also be used indirectly over the BGAN connection if there is intelligent user equipment connected to the UT that is accessible remotely by virtue of its PDP context. The user equipment can then be remotely commanded to issue AT commands across its local Ethernet connection to the UT.

If the terminal has entered either of the two power saving modes, Wake on LAN or GPIO, it cannot be commanded remotely. The terminal will be woken up when it receives a packet on its local Ethernet port unless the terminal is being kept in power down by the GPIO feature in which case the voltage being used to maintain the mode must be removed.

The next three sections give an overview of the configuration options for the three basic commanding methods and where to find detailed information:

- Using the Hughes WebUI Application
- Using AT commands
- Using SMS

6 Configuration via the WebUI

The UT is typically configured via the Web User Interface (UI).

The Web User Interface (UI) can be accessed from a local PC browser by entering 192.168.128.100 as the URL (unless you change the IP address of the UT). The WebUI can be used with IE7, IE8, Mozilla or Safari. If these browsers are not used then some features will not operate or be configured properly.

The following table shows the 9502 WebUI hierarchy:

Home	Connections	Settings	M2M	Security	SMS
Home	Manage Contexts Manage APNs	IP Address/DHCP Settings Ethernet Port	M2M Setup	Security	Send/Receive SMS Saved Drafts Sent Messages

Table 1: 9502 WebUI Layout

Details of how to use the WebUI are given in the Hughes 9502 Fixed Satellite Terminal User Guide (see RD.1).

Note that the WebUI will provide azimuth and elevation information for the appropriate satellite. It does not indicate which satellite has been selected.

7 AT Commands

The message set that is common to all BGAN M2M UTs is the set of M2M specific AT commands that are documented in the Hughes AT Command Reference document (see RD.2). The scope of the commands is as follows:

- Update of the UT firmware
- Update of the UT configuration file
- Scheduling power save mode
- Enable/Disable MAC address locking
- Setting the allowed MAC address list
- Set/Reset of UT passwords
- Enable/Disable UT facilities

- Enable/Disable remote SMS commands
- Send a file to a server
- Get firmware from the update server
- Get a file from a server
- Enable/disable remote access to the WebUI

Combinations of these commands are required to manage the UT. Appendix A of this document shows how these commands combine to support common activities (use cases) associated with management of the UT. These 'use cases' are:

- Performing a remote firmware update
- Setting up the UT security features
- Scheduling the power save mode
- Sending commands over SMS
- Remotely updating the UT configuration file
- Remotely accessing WebUI
- Retrieving a log file remotely

A full specification of AT Commands is given in RD.2.

8 SMS commands

The UT may also be configured by SMS commands and these commands may vary between manufacturers. The SMS commands supported by the Hughes BGAN M2M UT are shown in the table below. Note that the last command in the list, ATCO, enables the integrator to encapsulate specific AT commands into a SMS messages.

ACTIVATE	-	Activates a PDP context for the device(s) connected to the UT
DEACTIVATE	-	Deactivates some or all the PDP contexts for devices connected to the UT
CLEAR	-	Deletes SMS messages on the UT SIM card
GETINFO	-	Retrieves current information from the UT. This can be GPS fix information and/or communications information such as IMEI and carrier beam strength.
RESTART	-	Restarts the UT
WATCHDOG	-	Requests or modifies the current Watchdog settings
ATCO	-	Issues AT commands to the UT AT command handler which returns the response in an SMS. Not all AT commands are supported. See the Hughes 9502 SMS Remote Control Feature User Guide (RD.3) for the full list of supported ACTO AT commands..

All remote control messages and responses must fit in a single 160 character SMS.

The SMS handler automatically deletes any message that fills the last SMS slot in the USIM to ensure there is always room to receive control SMS messages. Control messages are received into the SIM then read out and deleted so a free slot is required.

Full details of using the remote SMS interface are given in the Hughes 9502 SMS Remote Control Feature User Guide (see RD.3).

Practical Guidance

9 Wake on any packet setup procedure

Introduction

Hughes has implemented a system that allows the 9502 M2M terminal to go in to a dormant state to conserve power. Although technically dormant, the UT does consume a very small amount of power while in this state: in the region of 10mw when supplied from a 12V DC source.

Unlike the Wake On LAN that can be found in PC motherboards that use a Magic Packet to bring the PC out of a dormant state, Hughes uses Wake On Any Packet (WOAP). This means the device connected on the LAN side does not need any intelligence or ability to use the Magic Packet protocol to wake the Hughes 9502.

There are 2 options to implement the WOAP feature:

1. Time of day timer. At a given time of day, the UT will shut itself down (web interface Settings / Ethernet settings)
2. Inactivity timer. A timer can be set so that should the LAN connection be quiet for a given period of time, the UT will shut down (web interface Settings / Ethernet settings)

Both of these methods are configurable via the 9502 WebUI.

Considerations in using WOAP

As mentioned, when the UT is in a dormant state it responds to any packet that the LAN interface sees. As the Ethernet protocol can be quite “noisy”, a number of steps need to be taken to ensure that WOAP works correctly.

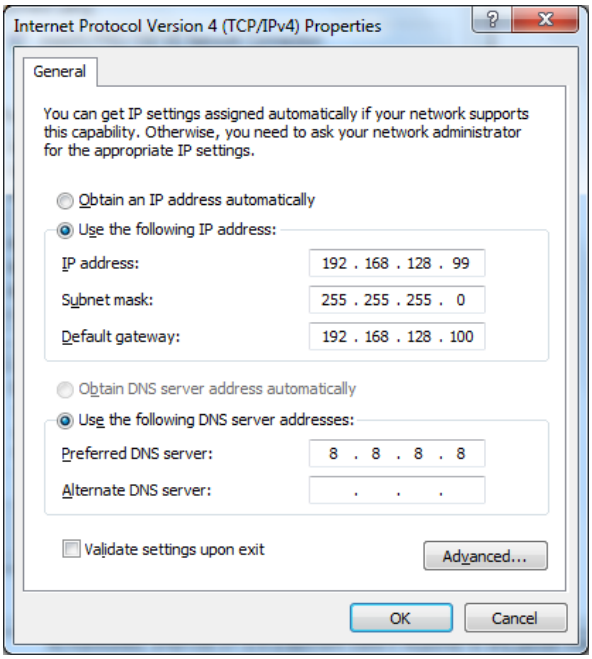
1. Set the LAN device to use a static IP address in the appropriate address range. Note that the DNS addresses for the LAN device to use will also need to be manually set, if needed.
2. Switch Off the DHCP server in the UT
3. Set the Always on Context in the M2M page
4. Set the Static IP Address given to the LAN Device in the M2M page
5. Switch Wake on LAN to ON on the Ethernet Settings page and configure the Time of Day or idle timer
6. Reboot the UT

Wake on any packet example using inactivity timer

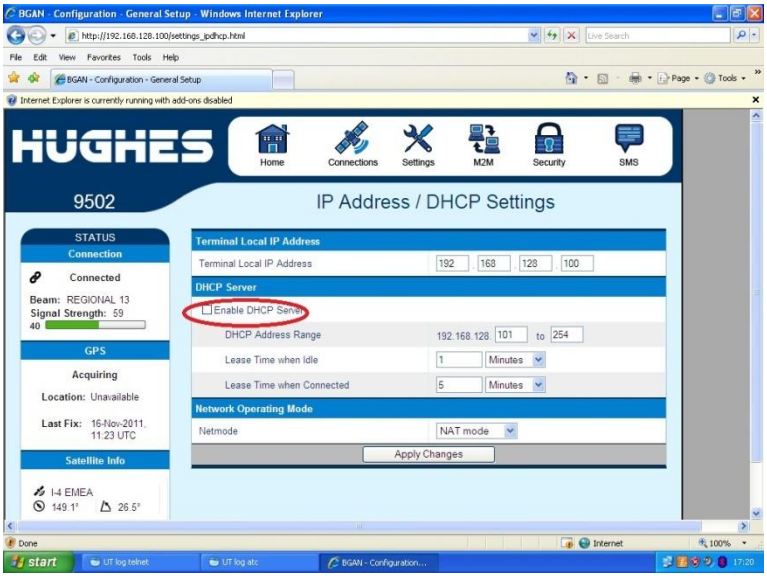
In this example, the LAN connected device is a MS Windows 7 PC connected directly to the UT with an Ethernet cable. It is possible that it is necessary to disable DNS on this PC otherwise it may periodically try to talk to the DNS server. Typically the end user will have a user equipment that is not a PC and probably will not require DNS.

The Hughes 9502 is to be configured for the subnet 192.168.128.0 /24 with the UT at 192.168.128.100, and the PC at 192.168.128.99. At some point the UT will ask to reboot. Do not reboot until the last step has completed.

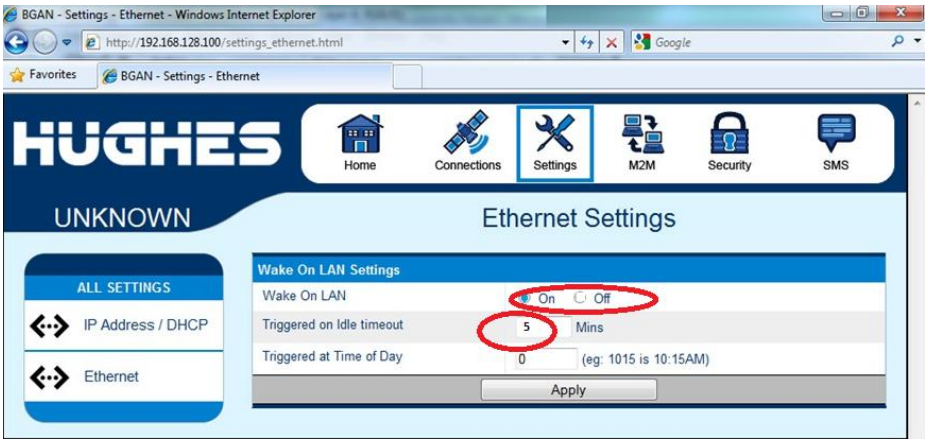
1. Configure the PC with an appropriate IP address in the LAN range.



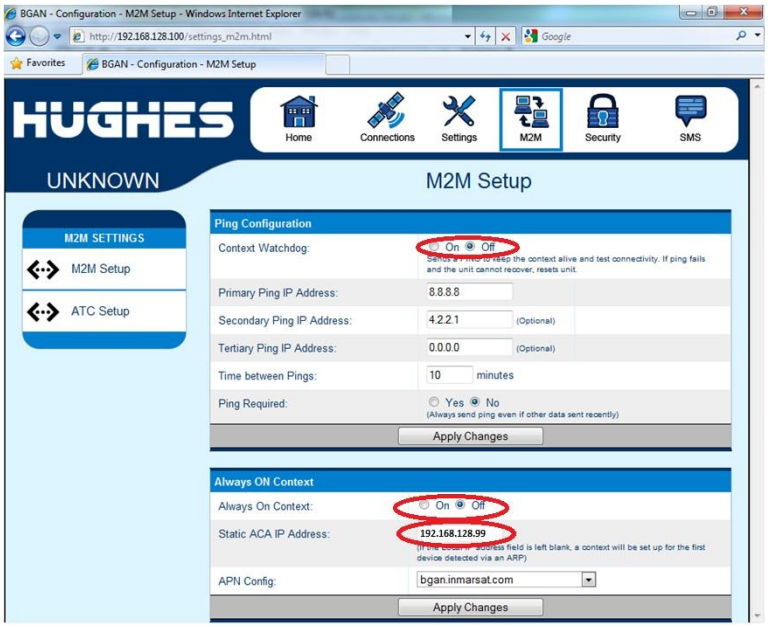
2. Log on to the UT on http://192.168.128.100 and select Settings and IP Address /DHCP option. Uncheck the Enable DHCP Server.



3. Go to the Settings / Ethernet page on the Web MMI and switch Wake on LAN to ON and the Inactivity timer to the required time, in this example 5 minutes, and press Apply.



4. In the M2M configuration page on the WebUI, set the Always On Context to Enabled and set the IP address of the LAN Device (in this case 192.168.128.99) in the Always On Context section / Static ACA IP Address. Also make sure that the Ping Configuration / Context Watchdog is disabled.



5. Reboot the UT. This can be done by the 'reboot now' option on the pop-up window after the configuration changes, or from the 'reboot' button on the Home page.
6. Close all applications on the PC.
7. After 5 minutes of inactivity, the UT will power down. Once it has powered down, you can open up a web browser to cause the UT to power up and it will be fully functional within 2 minutes.

10 Serial to IP operation

This section describes some practical experience of using serial to IP devices to connect emulated user equipment to the BGAN network using the Hughes 9502 as an access point. Testing was done using serial connections at 9600 bits per second with one stop bit and no flow control. At this speed, flow control was not an issue, but clearly it may become important if higher serial speeds are employed.

Satcom Gadgets Serial BGAN Interface

No problems were found with data communication in the simple checks performed. This was the only device checked to date that had a method of controlling the satellite terminal directly and should it lose its connection is able to reboot the terminal or itself.

In the version tested the SBI to satellite connection relied on DHCP to allocate an IP address to the interface. DHCP tended to be quite noisy on the LAN used to the extent that it would be incompatible with the 9502 Wake on LAN implementation.

Alphamicro Netport

It was possible to set a static IP address and a remote host that would be automatically connected when the device was activated. No problems were found with data communication in the simple checks performed.

This device had no concept of a satellite terminal so was not able to control the PDP context in any way so the M2M Auto Context Activation would need to be turned on and configured properly.

In our tests, it was possible to put the Hughes 9502 into power down (Wake on LAN) mode and wake it up with the Netport. The time taken between the Netport timing out due to lack of connectivity and the 9502 achieving full connectivity was about one minute. The 9502 took between one minute fifteen seconds and one minute forty-five seconds to activate a PDP context.

Digi International Inc One SP

This device accepts a static IP address and has an autoconnect function. No problems were found with data communication in the simple checks performed.

This device has no concept of a satellite terminal so was not able to control the activation of the PDP context and would need to rely on the Auto Context Activation within the 9502.

It was possible to put the Hughes 9502 into power down mode and wake it up with the One SP. The terminal timed out after 94 seconds.

Perle IOLAN DS1

This device has a number of different options/profiles that encompass Mobus, TCP and UDP. Checks were done using TCP. No problems were found with data communication in the simple checks performed.

It was possible to power down the 9502 using the device and the Wake up on LAN function was activated but the timeout was very short at 12 seconds. This left over a minute 30 seconds while the 9502 continued to boot and establish a PDP context.

General Comments

Timing is a significant consideration when using the 9502 terminal to connect user equipment to the BGAM M2M service. It is necessary to allow the terminal time to reactivate following Wake up on LAN before the user equipment starts to transmit data.

11 Using passwords

The default password for administrators is 'admin'. This password can be changed but it is important to make a careful note of the new password as this password is needed to reset the terminal.

There is also an SMS password that will be required for remote configuration of the terminal by SMS if this capability has been configured by WebUI. The default value of this password is 'remote'.

There is a security feature that will lock the terminal to the SIM using a PIN of up to 8 digits. If this is done then the PIN number will be needed before another SIM is used with the terminal.

The AT command port is locked by default and requires a password before the UT will respond to any AT commands. Use ***AT_ICLCK="AD",0,"<admin password>"*** where the admin password is *admin.*

For more details on these terminal security features see the Hughes 9502 Fixed Satellite Terminal User Guide (RD.1).

12 Accessing the Hughes WebUI remotely

This section describes how to access the 9502 WebUI remotely using IREMWEB operation via AT commands and SMS.

Using the AT command _IREMWEB the following occurs:

- A context is created for the UT
- A rule is created in the UT firewall to allow port 80 traffic only from the specified IP address range
- Unsolicited result codes are sent on AT interface or via SMS (see below)

For example, AT_IREMWEB=1,"98.150.120.0","98.150.120.254"

This allows computers with IP addresses in the range 98.150.120.0 to .254 to remotely access the WebUI. The second IP address is optional and if omitted only the specified single IP address can access the UT. For example, AT_IREMWEB=1,"98.150.120.17" allows only 98.150.120.17 to access the 9502 WebUI.

The IP address assigned to the UT PDP context is returned in an unsolicited AT command e.g. _REMWEB: 81, Global IP: 161.30.22.25

To access the WebUI, browse to this IP address. Note that each web page is about 500kBytes in release 5.9.1.3.of the terminal. This will be reduced to about 100kBytes by compression in future releases..

Note that the log files cannot be downloaded from the home page via IREMWEB because they use the wrong IP address and FTP is blocked by the terminal's firewall which blocks all traffic except HTTP to port 80 when accessing the UT Web UI remotely. Use _isendfile instead.

Network Address Translation (NAT) in the Distribution Partner APN may cause problems with IREMWEB. If the UT's global IP address is a private address, only hosts in the same domain may be able to reach it. Also, the IP address (or range) configured for the HTTP client must be that which appears on the network after any address translation. If the client host has a NAT-ed address, use www.whatismyipaddress.com to find the global IP address to use in the IREMWEB command e.g. ipconfig on the host shows private corporate IP address 10.130.25.147, but whatismyipaddress shows, 98.150.120.17, so use the 98 address in the IREMWEB command.

To tear down the context and end the remote web session: AT_IREMWEB=0

To achieve remote WebUI access with a remote management SMS do the following:

Send ATCO 2 remote _IREMWEB=1,"161.30.0.0","161.30.255.255" to allow HTTP access to the UT from any IP address in the range 161.30.0.0 - 161.30.255.255.

The response mode parameter in the command must be either '2' or '3' in order to get back a response SMS containing the global IP address that was assigned (dynamically) to the UT.

13 Troubleshooting

SMS processing logic

The UT SMS logic has a few parameter checks that it makes to determine if the received SMS message is a standard or a remote SMS control message.

- The logic checks the first word of the SMS to see if it is one of the recognized commands: ACTIVATE, DEACTIVATE, CLEAR, GETINFO, RESTART, WATCHDOG, or ATCO. These are all case-sensitive. If it passes this check then the message will be processed as a command message
- Next it looks for the password (case sensitive). If it passes the first check and fails the password check, then it sends an error message saying that the password is incorrect
- Once the first two validations pass, then it checks for the syntax and parameters. If the syntax or parameters are incorrect then it sends an error message

If a command SMS is not received from a sender on the “white list” when the “white list” is defined (see the WebUI security/remote SMS feature page/section), then the SMS is discarded with no response. The “white list” is a list of subscriber numbers that are authorised to send commands to the UT to prevent unauthorised access to the UT.

When SMS messages are received (regardless of type) they are stored in the SIM. They are then processed and depending on the message type or status they may be deleted.

For the 9502, if the first 4 characters of an SMS match any of the commands above (including case) it will be treated as a command message and will be deleted from the SIM after processing.

To ensure sufficient space in the SIM to receive command messages, when processing any SMS, if there are less than 5 slots available in the SIM the new SMS will be deleted regardless of its type.

13.1 SMS activate/deactivate messages

If an ACTIVATE SMS message is sent to a terminal and a PDP context is already active on the target unit’s PC of interest, that existing PDP context will be used and the ACTIVATE SMS will be discarded and no error will be reported back via SMS. The graceful way of handling a re-activation request remotely is to first send a DEACTIVATE SMS**,** wait few minutes and then send an ACTIVATE SMS with the updated QoS if required.

Due to inherent limitations in the Satellite Gateways and the SMS-protocol, the Remote-SMS commands and response SMS messages may sometimes take longer to get delivered and processed. While waiting for the Activation responses please exercise patience as they may take approximately 5-10 minutes for all the activation responses to reach their recipients. Please wait at least 10 minutes before re-sending Activation requests.

If a PDP context was setup manually for a PC of interest and the DEACTIVATE message is sent, that pre-existing PDP context will be torn down, even though it wasn’t established via an ACTIVATE command.

When the UT receives duplicate Activate or Deactivate messages and/or multiple messages:

- After reception of the first message, there is a 10 minute delay in the logic before a new message can be handled, so if the terminal receives multiple messages within that 10 minute delay after receiving the first one, the terminal discards the duplicate SMS message

  If the desired PDP session is already active and the UT receives another message to set up a PDP context for that same device, the UT will discard the SMS message as well

13.2 Other SMS issues

SMS commands must encode the ATCO command name in upper case e.g. ATCO not atco. If lower case is used the command will be treated as a regular SMS message rather than a command.

Generally, the format needs to be observed accurately and early usage has shown non-conformance with the format to have caused problems. For example, in the case of:

ATCO 3 password _IGETFW=.....

It is important that there are spaces between ATCO and the first number, between the first number and the password and between the password and the following field. This last space was frequently overlooked by early testers.

The Hughes terminal only accepts the underscore if it is encoded as ASCII hex 5F or GSM hex 11. Some devices have been known to encode it as 60 hex. There are a few ways to get around this: send the SMS from a Hughes terminal; force the sending device to use ASCII or GSM encoding.

When entering MSISDNs in the remote SMS white list the international dialling code should be represented using the + symbol for country access (or omitted). The local interpretation of the symbol ‘00’ for the UK will not work, therefore enter 8707721234567 or +8707721234567.

13.3 AT commands

Note that AT_ICLCK must be used to unlock AT command access because AT commands are blocked by default at terminal start-up. (This does not apply to ATCO remote SMS commands).

Appendix A: M2M Use Cases

In the following use cases, command formats have been specified using the following conventions:

- Where a command parameter is a string, the format indicates this by the use of double quotation marks (“). These quotation marks are required as part of the command sequence sent to the terminal. Usually this is stated explicitly in the format definition but in the case of facility it is specified in the definition of the parameter e.g. “RS”
- Where a parameter is a value, no quotation marks are used
- Angle brackets are used to mean that a value should be substituted to create the command sequence e.g. <mode> means that a value of 1 (for example) will be included in the sequence sent to the terminal. Where the value required is a string this is indicated by the format definition “<password>” for example and if in this case the password string is Inmarsat then the sequence sent to the terminal is “Inmarsat”

Note: For all AT commands issued in the examples (either issued locally or via an intelligent device that sends it to the UT over the local LAN interface), but NOT for remote SMS commands that encapsulate AT commands, it is first necessary to issue the following command in order to allow AT command operation:

_ICLCK Enable / Disable facility lock (this allows remote administrator access to the UT)

Example:

AT_ ICLCK=”AD”,0,“admin password”

Format:

AT_ ICLCK =”<fac>”,<mode>,”<admin password>”

Variables:

<fac>: “AD” for Administrator, “RS” for Remote SMS

<mode> : 0 = unlock, 1 = lock

This command must be re-issued after <u>each time the UT reboots</u> in order to restore AT command interaction.

14 Use case 1: Remote firmware upgrade

14.1 Summary

User updates the firmware (FW) file on a remotely located UT

14.2 List of actors

End user, remote M2M UT, Inmarsat server or customer FTP server, Inmarsat customer services team

14.3 Post conditions

Success state: UT firmware file replaced and in use

Failed end state: No change in UT firmware file

14.4 Trigger

Inmarsat informs the end user that a firmware upgrade is available

14.5 Sunny day use case

- After testing the new release on a local terminal, the end user decides to update the firmware version of a remote UT
- The operation is accomplished remotely; either by sending SMS commands or by AT commands from a local intelligent device that can be commanded remotely over a PDP context.
- The operation is a 2 step process:
    - The firmware file is downloaded from an Inmarsat server or the customer's own ftp site
    - The downloaded file is checked and then installed
- The user can specify deferred or automatic upgrade
- In deferred upgrade, after the firmware is downloaded the UT waits for a second message from the user before upgrading. Alternatively, the firmware is installed automatically as soon as it has been downloaded and passed an internal integrity check
- After upgrade, the UT returns a message confirming the new firmware is installed

14.6 Related AT commands

_IGETFW ***Get firmware file from update server & Load firmware either after file integrity check or explicit command from user.***

Example 1: Command the unit to download the latest firmware using defaults for all FTP and APN parameters. In this case, because the second parameter is “3”, up to two responses (SMS) will be received:

ATCO 3 rsmsPwd _IGETFW=0

Syntax:

AT_IGETFW=<mode>[,"<ftp_server>"[,"<ftp_uname>"[,"<ftp_passwd>"
[,"<apn>"[,"<apn_uname>"[,"<apn_passwd>"]]]]]]

N.B. *<mode> = Update mode*
0: Deferred update (requires supplementary _IUPDFW command before update is initiated)
1: immediate update after successful integrity check

N.B. *If <ftp server > value left blank, default Inmarsat server will be used.*
If <APN uname> value left blank, default free Inmarsat APN will be used.

_IUPDFW **Update firmware after file download**

Example:

AT_ IUPDFW=”bganx_5_9_x_x.bin”

Format:

AT_ IUPDFW=”<filename>”

_ICLCK **Enable / Disable facility lock (this allows remote administrator access to the UT)**

Example:

AT_ ICLCK=”AD”,0, “admin password”

Format:

AT_ ICLCK =<fac>, <mode>,"<admin password>"

Variables:

<fac>: "AD" for Administrator "RS" for RemoteSMS

<mode> : 0 = unlock 1 = lock

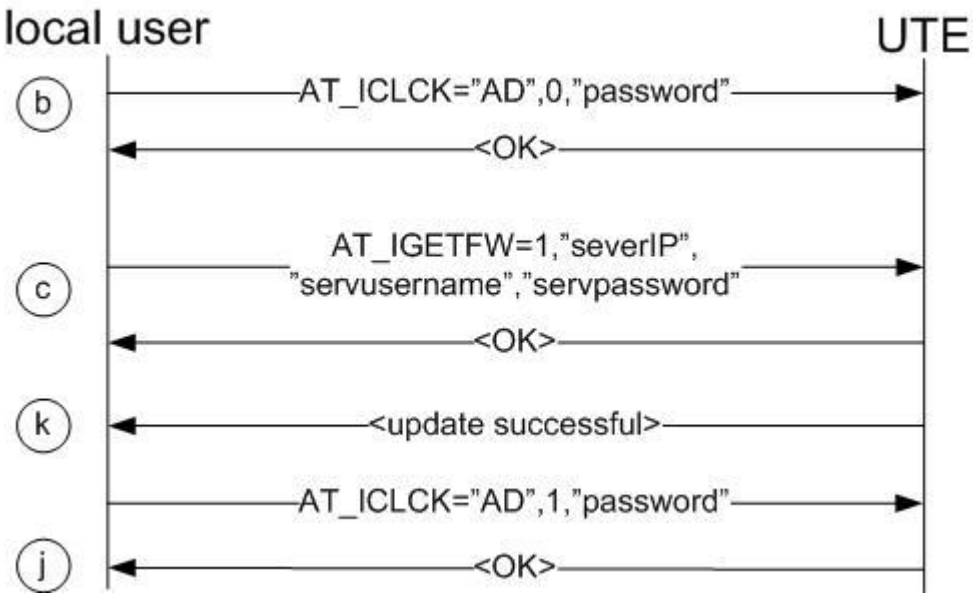
14.7 Main flow

14.7.1.1 Automatic firmware upgrade.

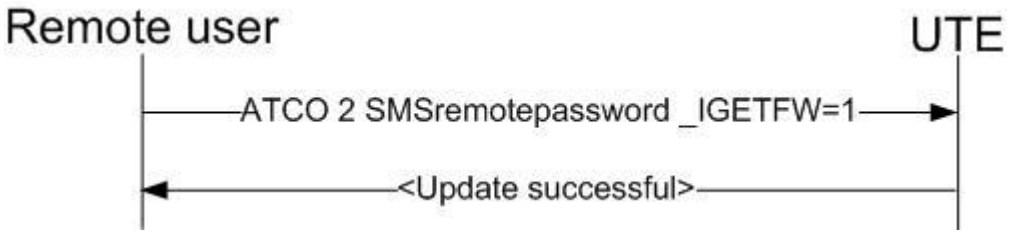
a. Inmarsat informs the user that a new M2M firmware version is available for download
b. End user enables remote administration access
c. End user initiates download of the new firmware by sending _IGETFW
   They indicate immediate upgrade in the _IGETFW command
d. UT establishes PDP context and connects to the Inmarsat server
e. Server authenticates the user's login details
f. UT browses to the Firmware file on the server
g. UT transfers the FW file
h. UT checks the integrity of the FW file
i. UT upgrades firmware
j. UT reboots to complete upgrade process
k. UT notifies user by SMS or AT of successful firmware update

14.7.1.2 Ladder diagrams

AT commands



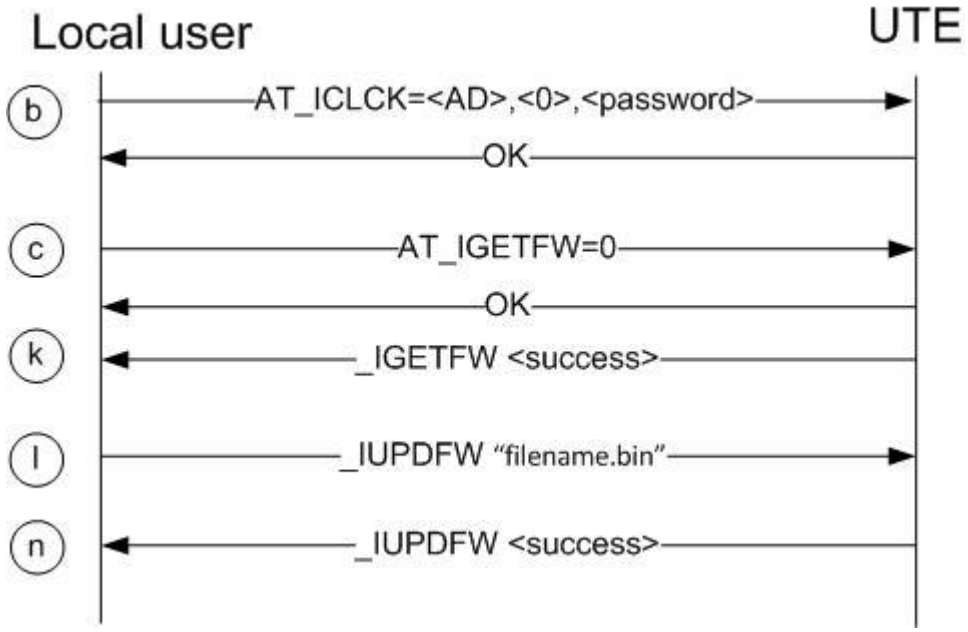
SMS commands



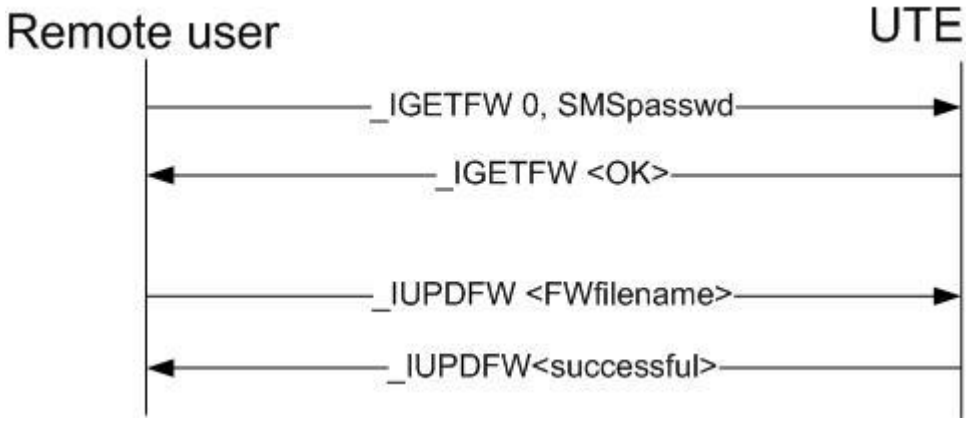
14.8 Deferred firmware upgrade

a. Inmarsat customer services inform the user that a new firmware version is available
b. End user enables remote administration access
c. End user initiates download of the new firmware by sending the _IGETFW command
d. They indicate deferred upgrade in the _IGETFW command
e. By choosing deferred upgrade, another explicit user command will be required to perform the update
f. UT establishes PDP context and connects to the Inmarsat server
g. Server authenticates the user's login details
h. UT browses to the Firmware file on the server
i. UT transfers the FW file
j. UT checks the integrity of the FW file
k. Because the user indicated deferred update in their _IGETFW command, the UT notifies user by SMS or AT indicating the result of the file downloaded
l. End user sends authorization to upgrade with _IUPDFW command , including firmware filename to use
m. UT upgrades firmware
n. UT responds to confirm success

AT command



SMS commands



14.9 Failure flow

UT will send an error message after any failure during the FTP download procedure. Refer to the Hughes 9502 SMS Remote Control Feature User Guide (RD.3) for error codes.

14.10 Assumptions

The UT is configured for SMS remote access and the user is sending SMS messages from one of the predefined MSISDNs.

When UT connects to the FTP server, it browses the directory of its model number to find the correct location for download.

The details of the Inmarsat download server and APN will be stored in the UT.

User employs the default Inmarsat FTP server and APN to download the new file, in both the illustrated cases above.

15 Use case 2 Setup UT security features

15.1 Summary

An end user has to implement their own set of configuration before they install and leave their UT to remote operation. A sub-set of these settings relate to security, they control who and how the UT can be accessed and manipulated, once installed.

15.2 List of actors

End user, UT

15.3 Post conditions

Success state: Access to the UT is limited to the desired extent

Failed end state: UT open to abuse or legitimate users locked out

15.4 Trigger

Ahead of installation, a user seeks to configure their M2M UT.

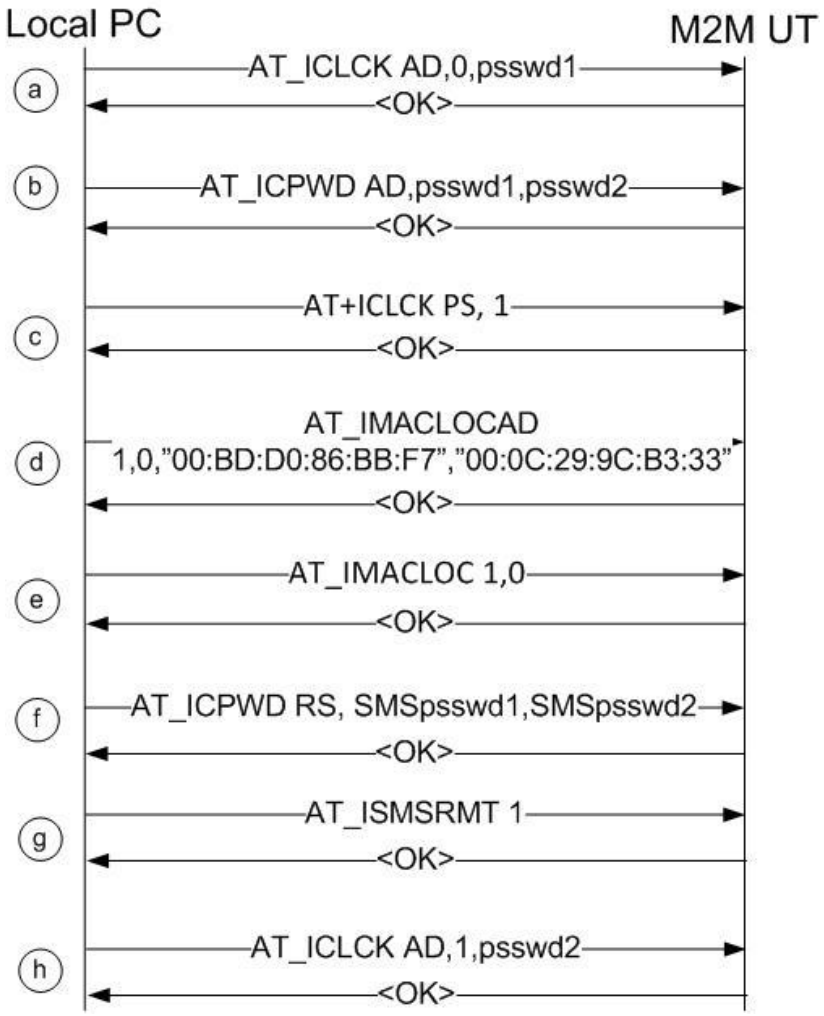
15.5 Sunny day use case

- Initially an AT command session is opened with the local UT
- The user specifies a new authentication password, to replace the default value.
  - This same password is used both to open future AT command sessions and provide administrator access to the WebUI.
- The user enables SIM to Phone locking in order to restrict use of the terminal to a single specific SIM. This locks the unique IMEI of the UT to a single IMSI
- The user specifies which equipment can connect to the UT:
  - MAC address filtering restricts the list of physically connected devices allowed
- The user specifies the mechanism for remote control of the UT:
  - Control via AT command and via WebUI is enabled at the beginning of each user session
  - Control by SMS command persists across power cycles and is likely to be setup during initial configuration
- Enabling remote SMS control for the first time is a 3 step process. The user must:
  - Specifies a new SMS facility authentication password
  - Specify the phone number (MSISDN) from which in-bound SMS commands can be received. The same MSISDN is also used as the recipient for SMS command responses or unsolicited messages
  - Enable the remote SMS facility
- The user closes their AT command session

15.6 Main flow

a. End user disables administration lock to AT session with ***_ICLCK***
b. Specifies new administrator password with ***_ICPWD***
c. Enables SIM to Phone locking with ***+CLCK***
d. Specifies white list of allowed MAC addresses with ***_IMACLOCAD***
e. Turns MAC address filtering on with ***_IMACLOC***
f. Specifies new SMS administration password with ***_ICPWD***
g. Enable remote SMS commands with ***_ISMSRMT***
h. End user enables remote administrator lock and closes the AT session with ***_ICLCK***

15.7 Ladder diagram



15.8 Related AT commands

_ICLCK **Enable / Disable remote facility lock** (see RD.2)

Example:

Enable remote administrator access to AT command sessions AT_ICLCK="AD", 0, "INMARSAT"

Format:

AT_ICLCK=<fac>,<mode>,"<password> "

Defined values:

<fac>

stands for facility

“AD” Administrator password for AT commands and WebUI (both features employ the same password)

“RS” Remote SMS password

<mode>

0 Unlock facility

1 Lock facility

<password>

defined by _ICPWD

_ICPWD Set or Reset facility password (see RD.2)

Example:

Set new remote SMS password to INMARSAT AT_*ICPWD=”*RS”,”HUGHES”,”INMARSAT”

Format:

_*ICPWD=*<fac>,”<old password>”,”<new password>”

Defined values:

<fac>

facility

“AD” Administrator password for AT commands and WebUI (both features employ the same password)

“RS” Remote SMS password

The default admin password is **admin**.

The default remote SMS password is **remote**.

_IMACLOCAD

Example:

_IMACLOCAD=1,0,”00:B0:D0:86;BB:F7”

Format:

_IMACLOCAD=<action>, <interface>, “<MAC Address>”[,”<MAC Address>”[,…]]

Defined values:

<action>

0 remove MAC address from white list

1 add MAC address from white list

<interface>

0 MAC locking over Ethernet

1 MAC locking over WLan (Note WLan is not available on M2M BGAN UTs)

_IMACLOC Enable / Disable MAC locking

Example:

Enable MAC address locking over ethernet AT_ IMACLOC=1, 0

Format:

_IMACLOC <status>,<interface>[,<interface>]

Defined values:

<status>

0 Disable lock

1 Enable lock

<interface>

0 MAC locking over Ethernet

1 MAC locking over WLan (Note WLan is not available on M2M BGAN UTs)

_ISMSRMT Enable / Disable remote SMS commands

Example:

Enable remote SMS commands AT_ISMSRMT=1

Format:

_ISMSRMT=<status>

Defined values :

<status>

0 Disable remote commands

1 Enable remote commands

16 Use case 3: Scheduled power-save mode

16.1 Summary

User puts their remotely situated UT into scheduled power-save mode.

16.2 List of actors

End user, remote UT

16.3 Post conditions

Success state: Remote UT is placed in power saving mode

Failed end state: Remote UT remains in normal operation

16.4 Trigger

Our end user operates a remote installation where electricity is not supplied from the grid and therefore, efficient power consumption is a priority. They want to minimise the power consumption of their remote UT.

16.5 Sunny day use case

- The user decides to initiate power-saving mode, a feature which powers down all the components of the UT except some parts of the network interface
- The feature can be activated remotely through AT session or via SMS command but note that once active, the terminal will not respond to remote SMS commands
- When they enable the feature, the user specifies the length of time that the UT must have remained idle in normal power consumption mode
- Once the UT has remained idle for the time specified in the user's command it will enter power-save mode and the terminal will not respond to SMS commands
- The UT will only then power back up when it receives local network traffic from other devices physically connected as part of the installation
- The user can later disable the feature only when the UT is back in normal power mode, by resending the same command but with the length of time set as null (left blank)

16.6 Related AT commands

_IPWSAVSCHD scheduled power-save

Example:

AT_IPWSAVSCHD="WOL_STATUS",1	Enable power savings
AT_ IPWSAVSCHD="TOD_TRG",0130	Enter power save mode at 1:30 UTC
AT_ IPWSAVSCHD="IDLE_TRG",10	Enter power save mode after 10 minutes idle

Format:

_ICLCK Enable / Disable facility lock

Example:

AT_ICLCK AD, 0, “psswd” Disable facility lock (allowing administrator access)

Format:

AT_ICLCK <fac>,<mode>,<password>

Variables:

<fac>:

“AD” for Administrator “RS” for RemoteSMS

<mode> :

0 = unlock

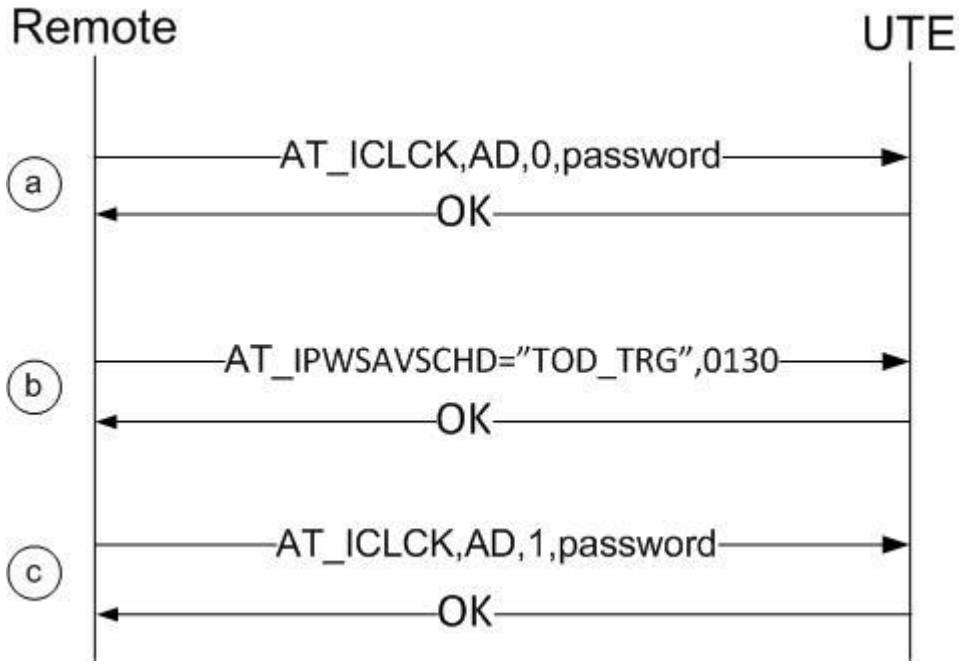
1 = lock

16.7 Main flow

a. End user enables remote administrator access
b. End user enables the feature and specifies the period of time the UT must be idle before going into power-save mode, by sending the command AT_ IPWSAVSCHD
c. End user disables remote administration access

16.8 Ladder diagrams

AT commands



17 Use case 4: Send commands over SMS

17.1 Summary

A user can configure their UT to be controlled via SMS commands. Control of some features available in a local AT session are available by encapsulating the required AT command within an SMS message of up to 160 characters. In addition a separate set of predefined SMS commands controls common settings.

17.2 List of actors

Remote end user, UT

17.3 Post conditions

Success state: AT command sent in SMS is auctioned by the remote UT

Failed end state: UT rejects command SMS

17.4 Trigger

The end user has a requirement to control their remote UT via SMS commands. This may be a backup or primary means of control.

17.5 Sunny day use case

- User wants to enable remote WebUI access for a specific IP address using an SMS
- During initial configuration, the user has set the UT to accept SMS commands. This included specifying an access password and defining the white list of MSISDNs from which SMS commands can be received. (See use case: Set up UT's security features)
- It is not necessary to specifically open an AT session in order to start
- User sends the ACTO remote SMS message from a predefined MSISDN
  The AT IREMWEB command is encapsulated within an SMS along with the SMS password
- The OK response to acknowledge a command is not sent back to the user in an SMS
  The UT will only send a response via SMS when:
  - the AT command generates an unsolicited response (e.g. a CME error code)
  - or the IREMWEB command is accepted for processing by the UT, in which case the response SMS will contain the global IP address to which remote web browsing is supported.
- The user can open a browser and accesses the remote UT's WebUI from the defined IP address as a result of this example command.

17.6 Related AT commands

See use case: "Set up UT's security features" for details of:

_ICPWD	*allows facility lock password to be changed*
_ISMSRMT	*facility lock for SMS commands and specifies allowed MSISDNs*
_IREMWEB	enable/disable remote access to WebUI over SMS

Example:

ATCO 3 HUGHES _IREMWEB=1,”161.30.180.212”

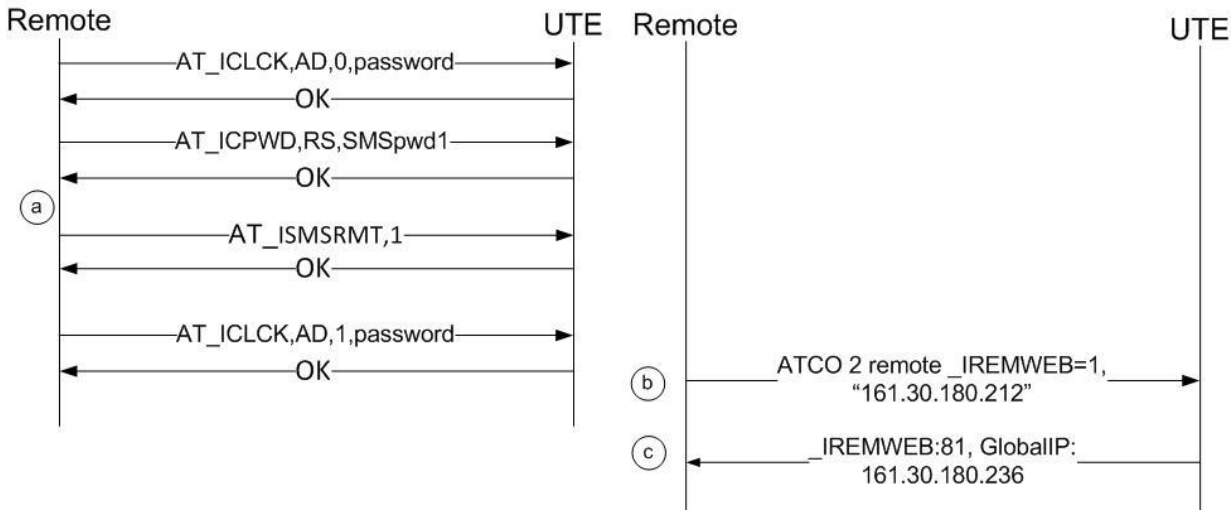
Format:

<SMS AT command prefix> <SMS command response parameter><SMS remote password>_IREMWEB=<mode>,”<ip address of end user pc>”

17.7 Main flow

a. Prior to installation, the end user enables remote SMS command access with ***_ICPWD*** and ***_ISMSRMT***
b. End user sends an SMS from predefined MSISDN including the ***_IREMWEB*** SMS command including their IP address
c. Remote UT returns the Global IP address to use in order to remotely access the webUI

17.8 Ladder diagrams



17.9 Assumptions

Once SMS command facility lock is enabled or disabled this state persists across power cycles. Assumption is that facility lock is disabled.

SMS commands can be sent and received when the UT is registered on the regional beam, a PDP context is not required to send and receive SMS messages

Due to inherent limitations in the Satellite Gateways and the SMS-protocol, the Remote-SMS commands & response SMS messages may sometimes take longer to get delivered and processed

Multiple command messages are queued upon receipt by the UT

18 Use case 5: Remote configuration file update

18.1 Summary

User updates the configuration file on a remotely situated UT.

18.2 List of actors

End user, remote UT, local UT

18.3 Post conditions

Success state:	Remote UT configuration file replace
Failed end state:	No change in UT configuration file

18.4 Trigger

The end user wants to update a remote UT with a copy of the configuration file that he has verified on a local M2M BGAN. The user uploads the configuration file to their FTP server.

18.5 Sunny day use case

- The user commands the remote UT to download a configuration file from a specified FTP server
- After integrity check of new file, the UT reports successful download
- User commands the UT to update, specifying configuration file name
- The UT checks the integrity of the configuration file
- UT reboots and loads the new file
- Finally, the UT returns a message confirming change to the new configuration file

18.6 Related AT commands

_IGETFILE Get file from server

Example:

AT_IGETFILE=”9502”,”config09092011.cfg”,”/tffs0”,”168.128.105.25”,”username”,”password”,[<APN name>[, <APN username>, <APN password>]]

The arguments after “password” are optional

Format:

AT_IGETFILE=”<ftp directory>”,”<filename>”,”<ut directory>”, “<ftp server>”,”<ftp username>”, “<ftp password>”[, <APN name>[, <APN username>, <APN password>]]

The arguments after “password” are optional

_IUPDCFG Update configuration file

Example:

AT_ IUPDCFG=”config09092011.cfg”

Format:

AT_IUPDCFG =”<filename>”

_ICLCK **Enable / Disable facility lock (this allows remote administrator access to the UT)**

Example:

AT_ICLCK=”AD”, 0, “password”

Format:

AT_ICLCK=<fac>,<mode>,”<password>”

Variables:

<mode>

0 = unlock

1 = lock

<fac>:

“AD” for Administrator

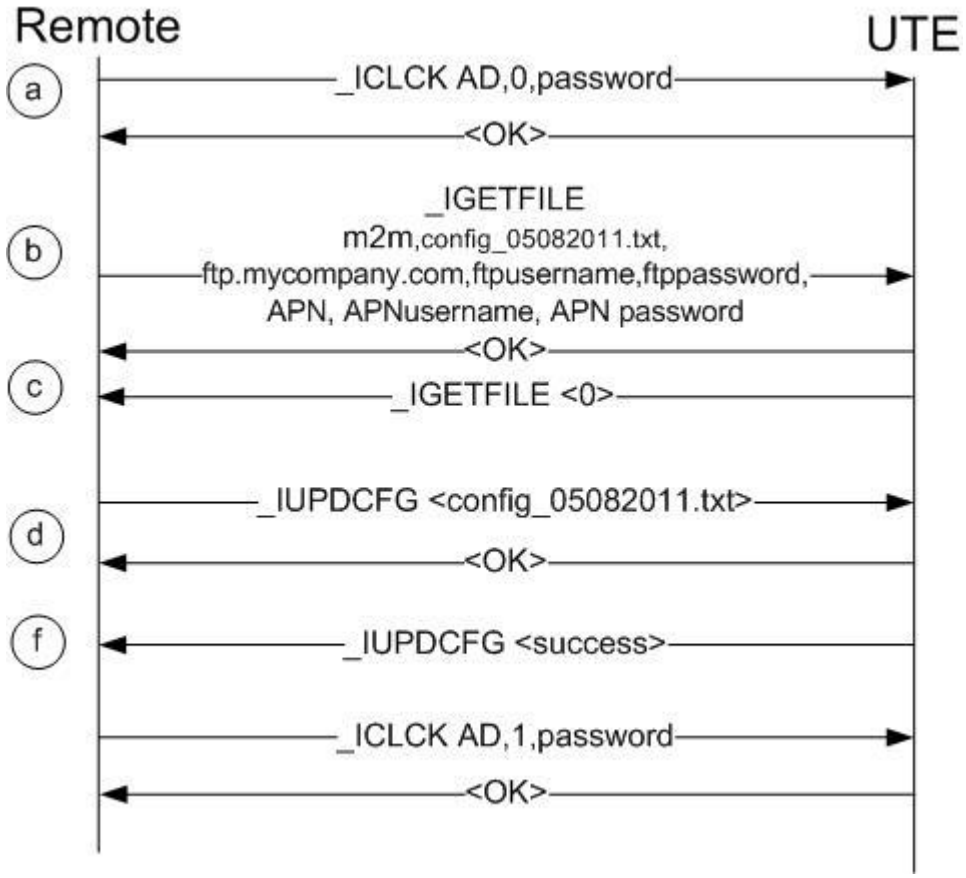
“RS” for Remote SMS command

18.7 Main flow

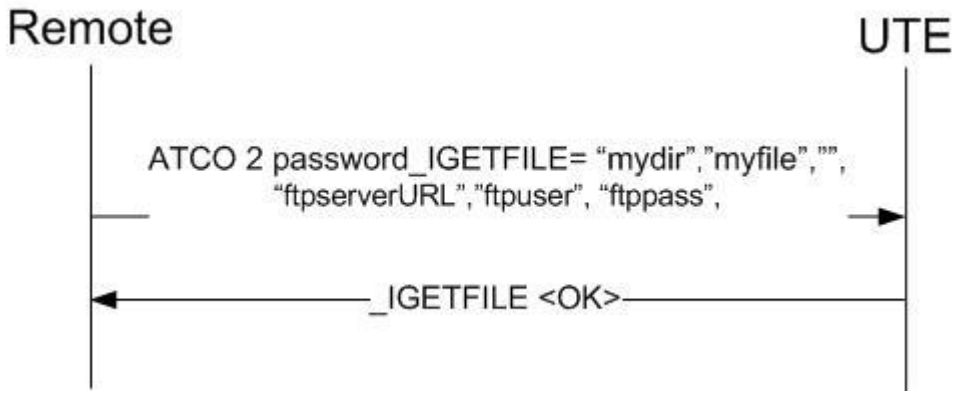
a. End user enables remote administrator access
b. End user specifies the file to download to the UT _IGETFILE
c. UT establishes PDP context and downloads the specified file and confirms
d. End user identifies the required configuration file and sends _IUPDCFG to remote UT. The command includes the alphanumeric file name of the locally stored file
e. UT performs successful integrity check on the configuration file
f. UT reboots to ensure that the configuration settings are loaded. UT confirms change

18.8 Ladder diagrams

AT commands



SMS commands



Failure flow

Any failures are communicated via unsolicited responses. Refer to the Hughes 9502 SMS Remote Control Feature User Guide for the list of result codes.

19 Use case 6: Remote WebUI access

19.1 Summary

By enabling remote access to the WebUI, a user can control their remote UT from an Internet browser installed on their local PC.

19.2 List of actors

End user, remote UT

19.3 Post conditions

Success state: The remote UT is configurable through WebUI on a PC local to the user

Failed end state: UT is not configurable through the WebUI

19.4 Trigger

End user decides to access the WebUI of their remote M2M BGAN terminal

19.5 Sunny day use case

- An end user wants to amend the configuration of their remote UT, using the WebUI
- A single command enables access and specifies the IP addresses which are allowed to access the UT. This security measure limits access to the UT only to identified PCs. The functionality can be set in an AT command session or via SMS command
- On their local PC, the user opens their Internet browser application and enters the IP address of the remote UT. They can now view all the settings configured on the remote UT
- Before they can edit any configuration, the user must input the Administrator code in the security section of WebUI

19.6 Related AT commands

_IREMWEB enable/ disable remote access to WebUI

Example:

Allow remote WebUI access to range of IP addresses
AT_IREMWEB=1,”161.30.105.4”,”161.30.105.16”

Format:

_IREMWEB=<mode>,”<ip address>”,”<ip address>”

Variables:

<mode> :

0 = deactivate

1 = activate

_ICLCK enable / disable facility lock

Example:

AT_ICLCK=”AD”,0, “psswd” Disable facility lock (allowing administrator access)

Format:

AT_ICLCK=<fac>,<mode>,”<password>”

Variables:

<mode> :

0 = unlock

1 = lock

<fac>:

“AD” for Administrator

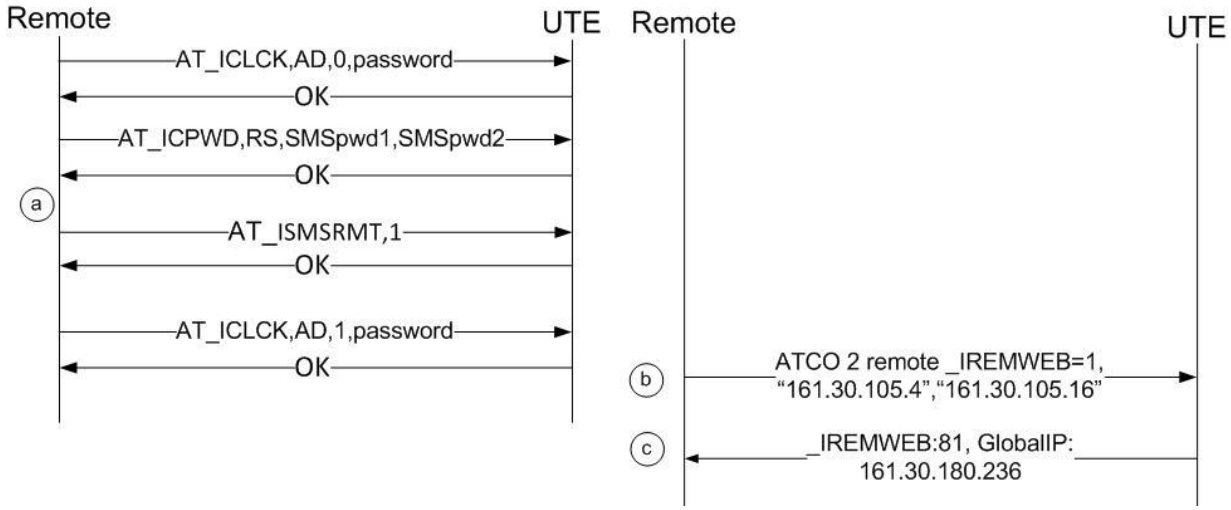
“RS” for Remote SMS

19.7 Main flow

a. The end user enables remote administrator access over AT command
b. He enables remote web access to the UTs WebUI and specifies a range of allowed IP address with _***IREMWEB***
c. The end user disables remote administrator access over AT command
d. The UT sends an unsolicited response with the UT IP address. This is sent to the AT or SMS interface depending on where the command came from

19.8 Ladder diagrams

AT commands and SMS Commands



20 Use case 7: Retrieve log file remotely

20.1 Summary

User retrieves log file from a remotely situated UT.

20.2 List of actors

Remote end user, UT

20.3 Post conditions

Success state: UT Log file retrieved

Failed end state: UT log file not retrieved

20.4 Trigger

Remote user requires UT log file

20.5 Sunny day use case

- The end user decides to upload UT log file
- The operation is accomplished remotely; either by sending SMS commands or by opening an AT session with the remote UT
- The operation is a 2 step process:
    - The user commands the UT to upload the log file to an FTP server using the correct file name
    - The UT returns a message confirming upload of the log file
- In this example, the message exchanges start with the user incorrectly specifying a filename so that the error handling can be illustrated

20.6 Related AT commands

_ISENDFILE Send file to server

Example:

AT_ISENDFILE=”/ram0”,”syslog.log”,”testdir”, 161.30.105.72,”testuser5”,”Inmarsat”, [*<APN name>[, <APN username>, <APN password>]]*

The arguments following “Inmarsat” are optional

Format::

AT_ISENDFILE=”<UT directory>”,”<ut log file name>”,”<ftp directory>”,”<ftp server>”,”<ftp username>”, “<ftp password>”[, <APN name>[, <APN username>, <APN password>]]

The arguments following “<ftp password>” are optional

_ICLCK Enable / Disable facility lock

Example:

AT_ICLCK=”AD”, 0, “psswd” Disable facility lock (allowing administrator access)

Format:

AT_ICLCK=<fac>,<mode>,”<password>”

Variables:

<mode> :

0 = unlock

1 = lock

<fac>:

“AD” for Administrator

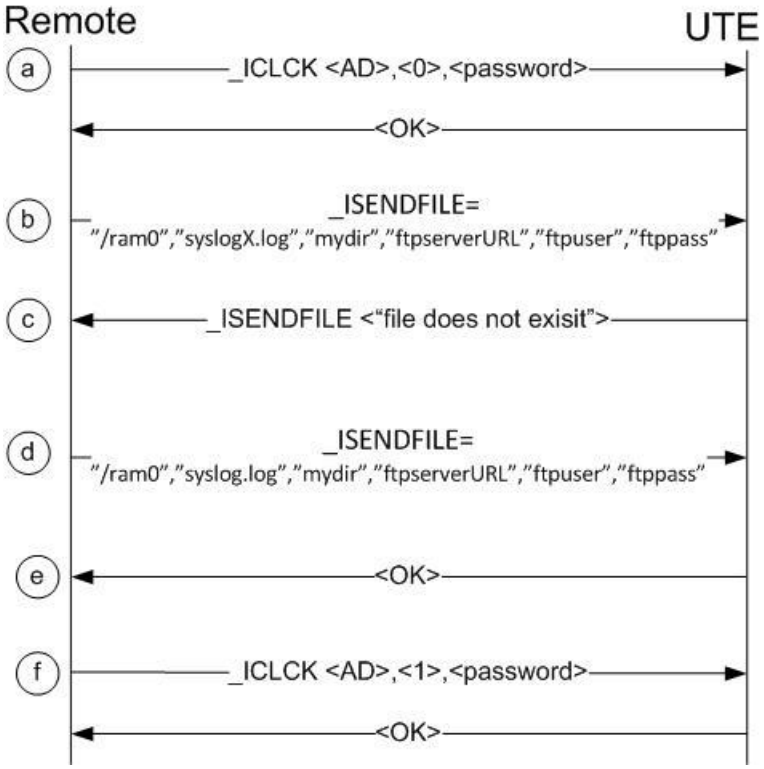
“RS” for Remote SMS

20.7 Main flow including error handling

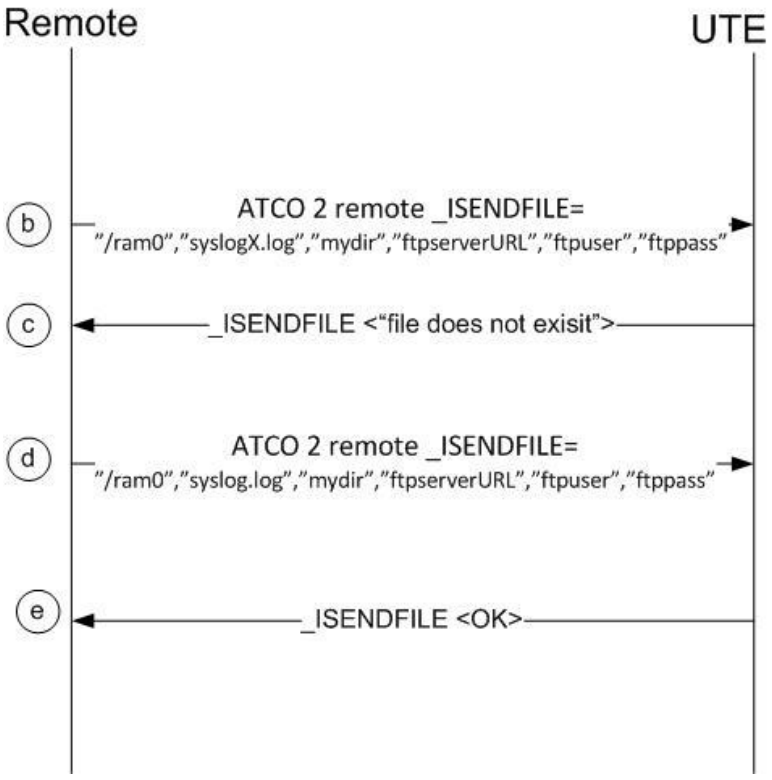
a. End user enables remote administrator access
b. End user specifies the file to upload from the UT with _ISENDFILE. They use the wrong filename (this is to demonstrate error handling only)
c. UT responses with an error message “File does not exist”
d. End user specifies the file to upload from the UT with _ISENDFILE with the correct filename
e. UT establishes PDP context and uploads the specified file. UT sends confirmation of upload
f. End user disables remote administrator access

20.8 Ladder diagrams

AT commands



SMS commands



20.9 Failure flow

Any failures are communicated via unsolicited responses. Refer to the Hughes 9502 SMS Remote Control Feature User Guide for the list of result codes.