GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

ALWAYS EVERYWHERE

Manual and Best Practices for Inmarsat Services from Geoborders

First Edition March 2008, current Revision November 2012.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Geoborders is an independent Mobile Satellite Communications Provider established in 1995. Geoborders is a Service Provider of Inmarsat services—including FleetBroadband, BGAN, SwiftBroadband, and Fleet. It is now one of the leaders in different commercial sectors and have a wide variety of clients worldwide, including individual travelers, large corporations, aid agencies, shipping companies, government departments and the military.

Select from a range of services to meet your remote communications requirements – whether on land, sea or air.

BGAN

BGAN from Geoborders provides high-speed IP data (up to 492 kbps), up to 384 kbps IP streaming, as well as voice, ISDN and fax. Ideal for portable, remote communications for the remote worker, media, first responder, and government / military users.

FleetBroadband

Bring the office to the ocean with high-speed IP data access, e-mail, Internet and crew calling. Geoborders is the world's leading FleetBroadband provider.

SwiftBroadband

SwiftBroadband from Geoborders delivers unprecedented high-speed data services for both the cockpit and cabin virtually anywhere in the world.

BGAN M2M

BGAN M2M is an evolution of the existing BGAN hardware and service providing a new generation of services designed specifically for low data rate SCADA applications.

Fleet

Having evolved from the highly successful Inmarsat A, B and M systems, Fleet from Geoborders provides high-bandwidth IP to maritime users from lightweight, compact, stabilized antennas.

Inmarsat C

Inmarsat C from Geoborders is a reliable two-way packet data service using compact, low-cost terminals. Access a broad range of Inmarsat C services from Geoborders.

IsatData Pro

IsatData Pro from Geoborders delivers low data rate communication over Inmarsat's I4 L-band satellite constellation for customers in remote and harsh environments.

Global Handheld Satellite Phone (IsatPhone Pro)

Inmarsat's new global handheld satellite phone, the IsatPhone Pro, takes advantage of the world's most advanced satellite communications network to provide exceptional quality and reliability.

Swift64 & Classic Aeronautical

Swift64 from Geoborders – our Mobile ISDN and Mobile Packet Data services – supports the full range of ISDN and IP connections for government aircraft, commercial aircraft passengers, corporate users and the flight deck.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

INDEX

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

1.| INMARSAT® Network Overview.

1.1| INMARSAT In-orbit Infrastructure and Coverage Maps

Inmarsat operates using the spot-beam capabilities of the latest generation Inmarsat-4 satellites. Three satellites are deployed to provide global coverage located at 25°East, 143.5°East and 98°West as shown below in Figure 1.

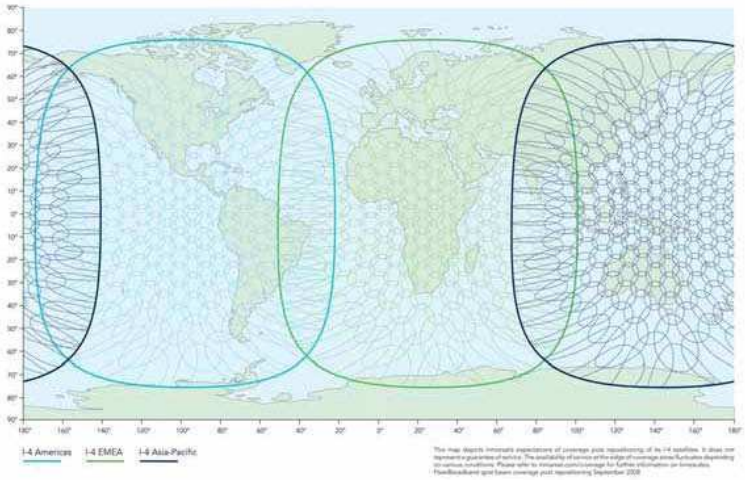


Figure: Inmarsat-4 Broadband Global Coverage (as at 18th Feb 2011)

The use of spot beams enables Inmarsat to re-use spectrum across the coverage area which, combined with the Dynamic Network Management, described below in Section 2.7, enables Inmarsat to optimise the use of satellite resources for all users connected to the network.

GSPS (IsatPhone Pro, LandPhone and FleetPhone) use the same INMARSAT Satellite but with a different technology and power, so coverage aria is slightly different.
The following map depicts Inmarsat expectations of coverage, but do not represent a guarantee of service because: the availability of service at the edge of coverage fluctuates depending on various conditions.

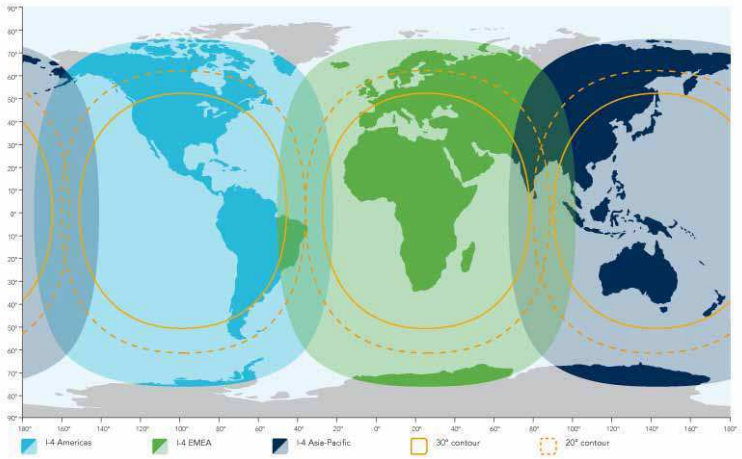


Figure: Inmarsat-GSPS Global Coverage (as at 1st June 2010)

1.2| Inmarsat Terrestrial Infrastructure

infrastructure which comprises five principle elements as shown below in Figure 2 and as described in the following sections.

- Satellite Access Stations (SAS)
- Regional Hubs or Points of Presence (PoPs)
- Network Operations Centre (NOC)
- Satellite Control Centre (SCC)
- Business Support Services (BSS)

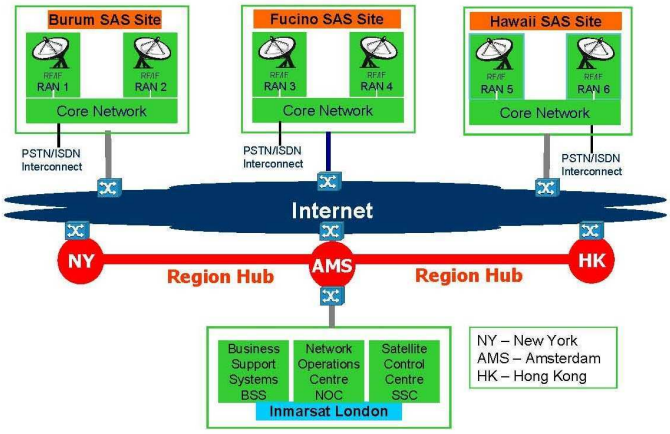


Figure: Inmarsat Terrestrial Infrastructure

1.2.1 Satellite Access Stations (SAS)

The three Satellite Access Stations provide the communications link/interface between each of the Inmarsat 4 satellites and terrestrial communications networks. Each SAS is owned and operated by Inmarsat, has an antenna for communication with the Inmarsat-4 satellites and direct connectivity to the PSTN, ISDN and Internet.

1.2.2 Regional Hubs or Points of Presence (PoPs)

The Regional Hubs (or PoPs) are the gateway to the Inmarsat global packet data network. The physical connection point within the hubs is referred to as a Meet Me Point and, while access is provided principally for Geoborders Branches, access to the Meet Me Points can also be provided for end-users by arrangement with your Local Geoborders Branch.
The regional hubs are owned and operated by third parties on behalf of Inmarsat and are currently operated by Telx in New York, Telecity in Amsterdam and HKCOLO in Hong Kong.

1.2.3 Network Operations Centre (NOC)

The NOC is located at Inmarsat HQ in London and provides resource and network management for the whole of the Inmarsat network worldwide.

1.2.4 Satellite Control Centre (SCC)

The SCC is also located at Inmarsat HQ in London and is responsible for the monitoring the health of the Inmarsat satellites, satellite attitude and orbital control and undertaking any maintenance work that may be needed on any of the satellites.

1.2.5 Business Support Services (BSS)

Business operations are also located at Inmarsat HQ in London providing all of the Business Support Systems required by the Inmarsat system including billing data, fault management and customer care.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

1.3| Inmarsat User Services and Airtime Plans

Inmarsat has developed a new advanced series of networks providing different sets of services (same network support multiple services). Advanced services are provided via distribution partners but the satellite gateways are owned and operated by Inmarsat directly; these new services are:

- GSPS – Fixed (LandPhone & FleetPhone) and Mobile (IsatPhone Pro) Phones.
- BGAN – Inmarsat Land/Mobile Voice & Broadband
- FLEET Broadband – Inmarsat Marine Voice & Broadband
- SWIFT Broadband - Inmarsat Airplane Voice & Broadband

1.3.1. GSPS – Fixed (LandPhone & FleetPhone) and Mobile (IsatPhone Pro) Phones.

GSPS means: **Global Satellite Phone Services**: provides voice services at 4.8 kbit/s and medium speed fax/data services at 2.4 kbit/s through Fixed (LandPhone & FleetPhone) and Mobile (IsatPhone Pro) Phones; GSPS offers a competitive alternative to the handheld, fixed and maritime phone solutions now available in the marketplace. The services offer high-quality voice connectivity via small, affordable equipment - ideal for remote workers in the energy, mining, government, media and first-responder communities.

1.3.2. BGAN – Inmarsat Land/Mobile Voice & Broadband

BGAN means: **Broadband Global Area Network** "Broadband for a mobile planet™"
If your job takes you away from the office - even off the beaten track - BGAN can help you stay as productive as if you were back at base. Choose from a range of devices, for personal use or to network a team.
Make phone calls, Send and receive text messages at the same time as accessing data applications via a standard desktop phone, wherever you are on the planet.
(BGAN) is a new family of services and products operating at data rates up to 492 kbps. Using a lightweight satellite terminal, comparable to or smaller than the size of a laptop computer, enable users to access email, corporate networks and the internet, transfer files, video conference, and make telephone calls, from nearly anywhere in the world. BGAN operates using a new generation (I-4) of the most advanced communications satellites ever launched.
The I-4 satellites will provide the BGAN service on up to 228 narrow spot beams while simultaneously providing the legacy services on 19 wide spot beams.

1.3.3. FLEET Broadband – Inmarsat Marine Voice & Broadband

Fleet Broadband (FB): is a maritime service, Fleet Broadband is based on BGAN technology, offering similar services and using the same infrastructure as BGAN. A range of Fleet Broadband user terminals are available, designed for fitting on ships.

1.3.4. SWIFT Broadband - Inmarsat Airplane Voice & Broadband

Swift Broadband (SB): is an aeronautical service, Swift Broadband is based on BGAN technology and offers similar services. SB terminals are specifically designed for use aboard commercial, private, and military aircraft.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

2| Inmarsat Services

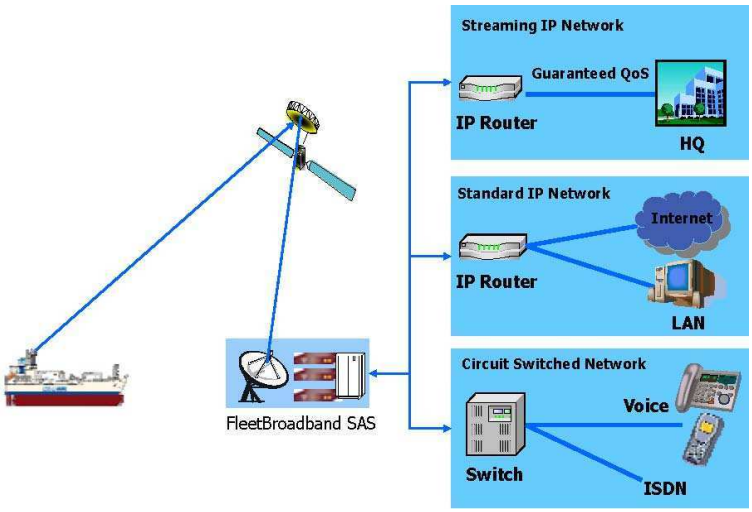
Inmarsat provides an on-demand range of services to suit all on-board applications. The system uses proven technology and the terminal is quick and easy to install and operate. And, unlike previous generations of Inmarsat terminals, services can be accessed and used simultaneously!

Voice	•4kbps circuit-switched service •Voicemail •Enhanced services: call waiting, forwarding, barring, holding •Broadcast quality voice
Data Standard IP	•High Speed Standard IP (NOT MPDS) •Variable bit rate service – Shared & Best Effort •Up to 432/432 kbps (send /receive)
Data Streaming IP	•On-demand guaranteed bit rate service •32, 64, 128, 256 kbps (send & receive) • ISDN legacy compatibility
Global Text	•Send and receive SMS

Figure: Inmarsat Services

One Device, Two Domains, Three Data Networks

Inmarsat supports two modes of data connection - circuit-switched and packet-switched (IP) data. And within the packet-switched IP domain two service levels exist – Standard IP (contended best-efforts) and Streaming IP (guaranteed QoS). So Inmarsat provides a total of three types of data connections, as illustrated in Figure 4 below, which means that you can select the data connection that is most suited to your needs and carries your traffic in the most cost-effective manner.



GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

2.1| VOICE - Direct Dial Voice Service

Inmarsat offers a direct dial voice telephony service using compression technology (the AMBE+2 codec3) delivering voice encoded at 4kbps (note that the 4kbps refers to the voice coding rate used by the AMBE+2 codec and should not be confused with VoIP). This makes efficient use of satellite capacity whilst delivering good speech quality.
It is possible to make a circuit-switched voice call whilst simultaneously using Standard and Streaming IP data services. Features of the direct dial voice service are:-

- Available on all Inmarsat terminals
- Landline quality speech (voice encoded at 4kbps)
- To and from:
  - Terrestrial networks
  - Mobile networks
  - Inmarsat terminal to Inmarsat terminal
- Can be used simultaneously with data
- Supports supplementary value-added services which are typically found on terrestrial networks such as:
  - Voicemail
  - Caller ID, Call Hold, Call Waiting
  - Call Forwarding, Call Barring
  - Short-code Dialling
  - Generic short-codes supported on the Inmarsat system are shown in Table 2 below

Short-Code	Action
12	Access to a DP's directory enquiry system
28	Access to a DP's ISP service
33	Access to a DP's customer service/technical help desk
36	Access to a DP's credit card calling system
94	Access to a DP's automatic loop back/test system

Table: Inmarsat Generic Short-codes

2.2 | VOICEMAIL - Voicemail Service

Inmarsat provides a voicemail facility which is comparable with that offered by most terrestrial mobile networks. A subscriber's service profile can be provisioned so that call forwarding will divert calls to the voicemail server whenever the subscriber is unable to receive incoming calls. Subscribers receive a notification via SMS that they have messages waiting for them.
In addition to the basic messaging service, subscribers can forward messages to another number, record a message and distribute it to one or more subscribers and access their voicemail from any telephone, fixed or mobile.

Voicemail is accessed via a short code on the Fleet Broadband network (57) or by dialling + 00 870 77200 1899 from any other network.

Voicemail is accessed via a short code on the GSPS network by dialling +870 772 001 899 from terminal or from any other network.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

2.3| SMS – Global Text

The Inmarsat network incorporates an SMS (text) messaging application with a full range of messaging features. The SMS message format follows the standard 160 character structure. Inmarsat does not support concatenated SMS.
You can send and receive SMS messages to and from other Inmarsat terminals and terrestrial cellular networks4 via your laptop or computer using the Inmarsat LaunchPad utility as shown below in Figure 5.

Figure: LaunchPad SMS (Text) Interface

2.4| STANDARD IP - Standard IP Data

The Standard IP data service provides up to 432kbps (maximum data rate will vary depending upon the type of terminal used) on a contended, best-efforts basis. There are no guarantees associated with this service. If the link is "busy", with many active users, then the observed bit rate will be lower than if the link is "quiet" with little traffic (see Section 2.7 below, entitled Inmarsat Dynamic Network Management for further details).
Standard IP is best suited to most typical office applications such as Internet browsing, e-mail, FTP and also numerous maritime applications such as electronic charts, weather updates, engine monitoring and many more. This is the type of connection that will be used most of the time and for most applications.

2.5| STREAMING - Streaming IP Data

In addition to Standard IP, for customers who require a guaranteed bandwidth, (and hence un-contended connection), one or more dedicated Streaming IP connections can be also be supported. Streaming IP provides an on-demand, guaranteed Quality of Service connection at any one of 32, 64, 128 or 256 kbps. The capacity is not offered to other users and effectively delivers reserved capacity for a specific IP connection (see Section 7.5.1 below, entitled About PDP contexts, for more information).
Streaming IP is available on demand and on a "first-come first-served" basis. If the channel requested is unavailable a user can request another channel with a lower bit rate.
Streaming is very important for time-critical data transmissions such as live video and audio but un-optimised resource-intensive enterprise applications like Oracle, SAP and database synchronisation can also benefit from the improved interactivity provided by Streaming IP. Further characteristics can be assigned to a Streaming IP link, including error correction and application-specific routing instructions.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Inmarsat offers streaming class connections at 32, 64, 128 and 256kbps. The actual data rate and maximum number of Streaming IP connections varies and depends upon the type of terminal used, link conditions, available capacity and elevation to the satellite.
streaming connection has a per minute tariff structure.

2.6| ISDN & FAX - Circuit-switched Data Services

Circuit-switched data services are available from the moment the terminal is registered to the network and data connections can be initiated from either the ship or the shore (unlike IP data connections which must be initiated from the ship).
ISDN: The Inmarsat network supports mobile-originated and mobile-terminated ISDN circuit-switched data calls at 64kbps. Inmarsat provides one 64kbps B-channel per terminal and both UDI and RDI are supported. A user may run simultaneous ISDN and Standard IP sessions1 but not simultaneous ISDN and Streaming IP sessions.
As with Inmarsat Fleet ISDN, two terminals may be bonded together to deliver 128kbps.

3.1kHz Audio2: In order to support **legacy modem and facsimile** users, Inmarsat provides PCM-coded 3.1kHz audio via a 64kbps transparent bearer. This service can be used to make and receive legacy modem, facsimile and speech calls requiring PCM coding to and from the terrestrial PSTN or ISDN and also supports encrypted voice such as STU III. The 3.1kHz audio service is provided at the terminal typically via either an RJ-11 analogue telephone connector or RJ-45 ISDN connector (where supported).
The propagation delay associated with satellite communications has been known to impair the performance of older fax machines but modern Group 4 machines tend to perform very well on a satellite circuit.
Not all circuit-switched data services are supported by all Inmarsat terminal types.

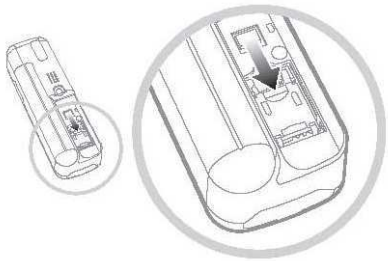
NOTE: ISDN and 3.1kHz audio services cannot be used at the same time as streaming data services.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

3| Best Practice Summary for IsatPhone Pro

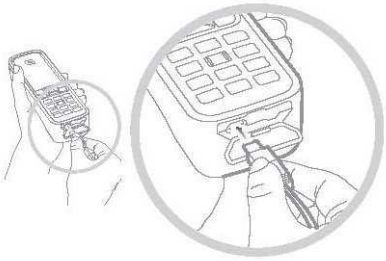
3.1| Insert the SIM card

- Remove the battery cover by using a coin to turn the screw slot until it is vertical.
- If the battery is in place, lift it out.
- Slide the catch down on the SIM holder and flip it outwards.
- Make sure the angled corner of your SIM card is on your left and slide it into the holder.
- Flip the holder back into place and slide the catch back up.
- Insert the battery, replace the cover and turn the screw slot until it is horizontal.



3.2| Charge the battery

Connect the charger to a power source and the micro USB connector to the port at the base of the phone.



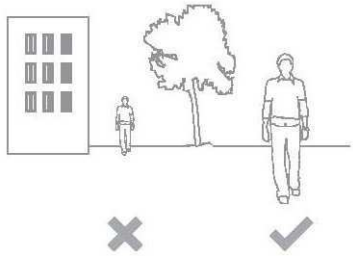
3.3| Switch on

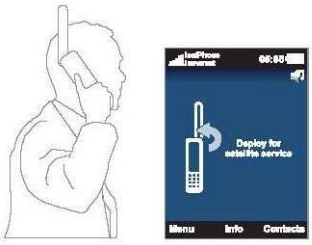
Hold down the red key until the screen lights up. The first time you use your phone, use the navigation keys to select your language and set the time zone. To switch off, hold down the red key until the screen shuts down.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

3.4| Connect to the satellite

Stand outside with a clear view of the sky and the phone antenna pointing upwards.
The top left of the screen will display 'Inmarsat' once you are connected to the satellite. At least 2 signal bars are required to make and receive calls.
Note: Before you make a call, your phone needs a GPS fix so it can be located by the satellite. This happens automatically, but if a new GPS fix is needed, the icon will be displayed. Place the phone in the open with a clear view of the sky until the icon disappears.





3.5| Make a call

Enter the full international number by dialling +, country code, area code (without the leading 0), telephone number and press the green key eg. +44 1621 123456 . To end a call, press the red key.

3.6| Answer a call

When your phone rings, press the green key . Remember, to receive a call, you must be connected to the satellite with the phone antenna pointing upwards.

3.7| Listen to voicemail

Hold down the key and you will automatically be connected to your voicemail. Alternatively, call +870 772 001 899 and press the green key .

3.8| PRE-PAY Balance and TOP-UP instructions

You can check for free your Prepay Balance dialling ***106#** and pressing the red key.
To redeem your top-up voucher you dial ***101*voucher number#** and press the red key for example if your Voucher is 1234567890123456 you will have to digit:
*101*1234567890123456#

3.9| Test your Satellite Phone calling for free +870.776.999.999

You can always test your satellite phone calling with no charge the test number:

+870.776.999.999 (Free Test your Phone!)

3.10| Description of your IsatPhone Pro

Please refer to the CD, which contains a full user guide and applications for contact synchronisation, firmware upgrades and USB drivers.
Also available at: http://geoborders.com/it/p/155

3.11| Installing the USB drivers on your Windows PC

Select software > USB drivers from the CD.
You will need to install the USB drivers on your PC before installing the contact synchronisation and firmware upgrade tools.
Installing the USB drivers also reduces your phone's charging time.
To install the USB drivers on your PC, perform the following procedure:

Select software > USB drivers from the CD.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Click Install.

The Software Installation dialogue box appears.

Click Continue Anyway. The Install Driver dialogue box appears.
Although the application has not passed Windows Logo testing, it is safe to continue with the installation. Proceed by clicking Continue Anyway.
Note: The Software Installation dialogue box may appear several times.
Click Continue Anyway every time it appears.

The drivers are successfully installed.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

3.12| Connecting the IsatPhone Pro to your Windows PC

PLEASE NOTE: do not connect your device before installing USB Drivers!

To install the new hardware, perform the following procedure::

Connect your IsatPhone to your PC with the
supplied USB cable. If your phone is not switched on, switch it on now.
When the USB cable is connected, the following pop-up will be displayed: 'New hardware found: IsatPhone Pro Composite Device.'
The Found New Hardware Wizard appears.
Select No, not this time and click Next.

Select Install from a list or specific location
(Advanced) and click Next.

Select Don't search. I will choose the driver
to install and click Next.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Click Next again.
The Hardware Installation dialogue box appears.

Click Continue Anyway.

The Found New Hardware Wizard installs
the software.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Click Finish.
The System Settings Change dialogue box appears.
Note: The installation procedure from Step 1 to Step 7 is repeated for other IsatPhone applications, eg. the fax modem interface, the contact synchronisation and firmware upgrade tools.
Disconnect the USB cable from your PC and
your phone.

Repeat the instructions from the beginning as many times as prompted by your PC in order to load each USB driver. On finishing, you may be asked to restart your PC for the changes to take effect. Click Yes. Your PC will automatically restart.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

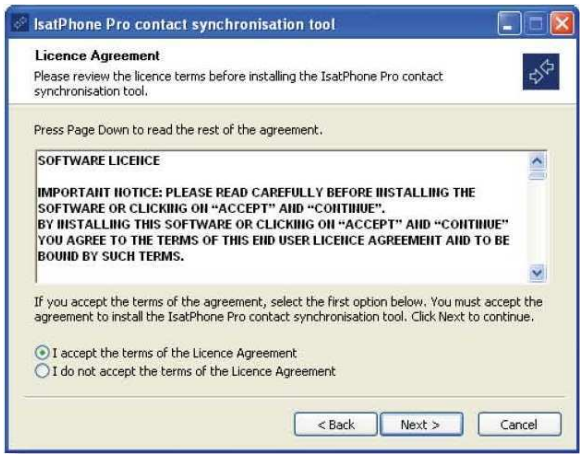
3.13| How to synchronise your contacts from Outlook

3.13.1 Install contact synchronisation tool

The contact synchronisation tool enables you to transfer contact information between your PC and your phone. The tool is compatible with Microsoft Outlook and Microsoft Outlook Express.
Please note that you need to install the USB drivers before installing the contact synchronisation tool.

Select software > contact synchronisation tool from the CD.
The IsatPhone Pro contact synchronisation tool setup wizard appears.

Click Next.



Read and select I accept the terms of the
Licence Agreement and click Next.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Click Install to begin the installation process.
Note: You can click Browse… to change the installation folder location.

Click Next after the installation process is complete.
Note: You can click Show details to display the installation details.

Click Finish.
The setup is complete.

Note: If Run the application is selected, the tool is launched once the setup is complete.

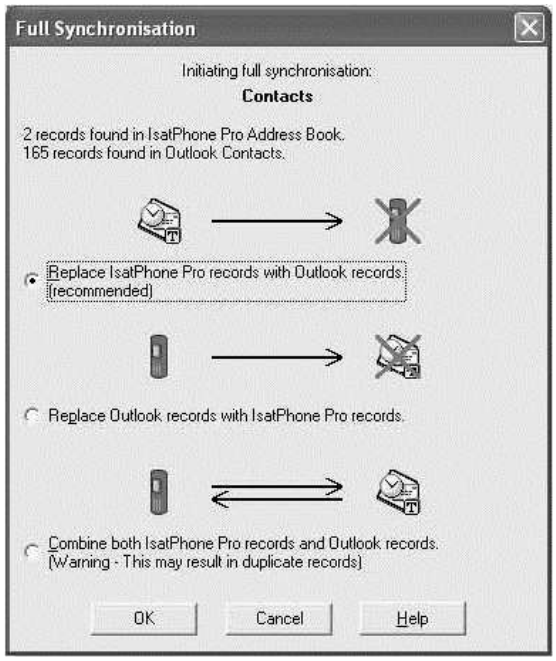
3.13.2 synchronising your contacts

Connect your IsatPhone to your PC with the supplied USB cable.
If your phone is not switched on, switch it on now.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Double-click the IsatPhone Pro contact synchronisation tool icon on the taskbar to run the tool or select Start > Programs > IsatPhone Pro > contact synchronisation tool > contact synchronisation tool.
Select Microsoft Outlook or MS Outlook Express to synchronise with your phone and click OK.

Click the Synchronise icon on your PC application. All the contacts in MS Outlook will be transferred in accordance with the option selected.
Note: Synchronisation settings can be set before synchronising. Please refer to the appendix.

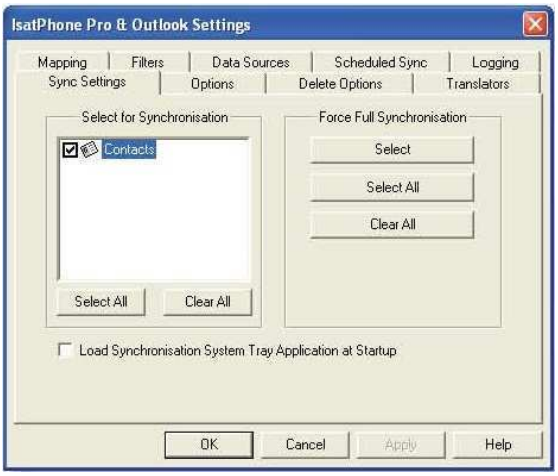


The first time your phone is synchronised with a PC, you will be prompted to select one of the following three options:
Replace IsatPhone Pro records with Outlook records. Selecting this option will delete the existing contacts on your phone and replace them with Outlook contacts.
Replace Outlook records with IsatPhone Pro records. Selecting this option will delete all Outlook contacts and copy all your phone contacts to the Outlook address book.
Combine both IsatPhone Pro records and Outlook records. Selecting this option will copy all the contacts from your phone to Outlook and vice-versa.
If your contacts have previously been synchronised, only changes will be updated.
Click OK.
After synchronising your contacts, disconnect the USB cable from your PC and your phone.
To customise synchronisation settings, please see next page.

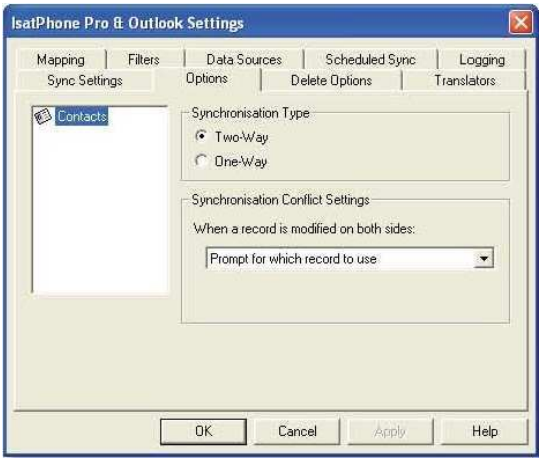
GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

3.13.3 Synchronisation settings.

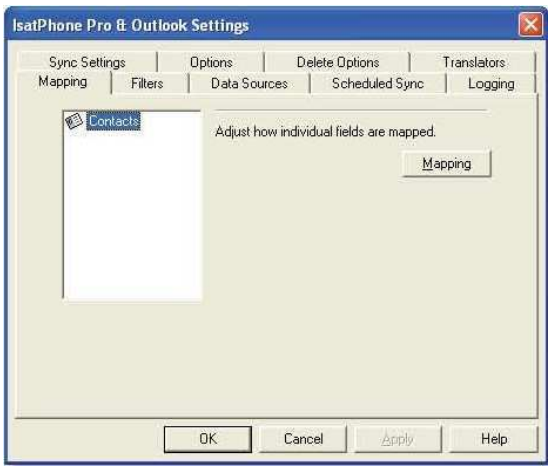
Select Tools > Settings or click the settings icon on your PC application to change the profile settings. The profile settings are explained below:



Sync Settings:
Select the source items you want to synchronise.

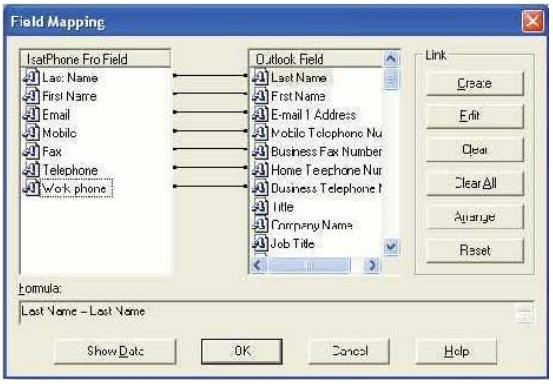


Options: You have the option of selecting either two-way or one-way synchronisation for your records.
Two-Way: changes on each side are reflected on the other. You also have the ability to specify what should happen when the record has been modified on both sides (a conflicting record).
One-Way: changes on one side take precedence over the other.



Mapping: To transfer data between your phone and the PC, a link must exist between the individual fields on both devices.
For example, the First Name field in Outlook
must be linked to the First Name field in your phone book.
The collection of links that tell the synchronisation software what to do with data is called Field Mapping.

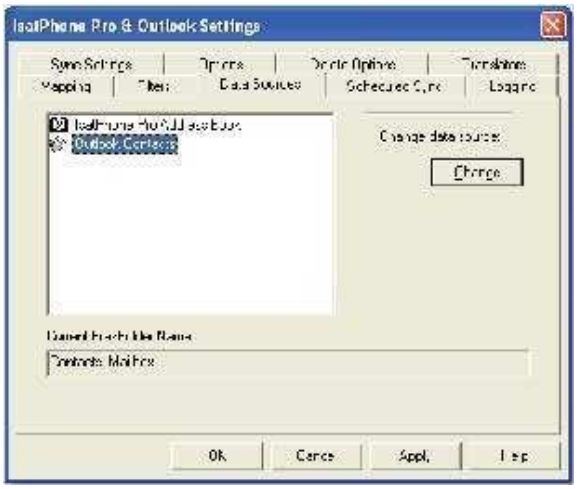
GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com



Click Mapping to view and edit the existing mapping of individual fields.
Note: When you first install the synchronisation software, default links are created for you.

Filters:
Filters are used to select only the contacts you need. This can speed up the synchronisation process by limiting the amount of data transferred.
Filters do not delete data from the side with the complete data set. If a record is created on the partial data set side that is not within the filter range, it will be synchronised to the side with the complete data set. On subsequent synchronisations, if this record remains outside the filter range, it will be deleted from the partial data set, but will remain in the complete data set.
The translator selected contains all records (the complete data set). The translator not selected will contain the smaller set of filtered records (the partial data set).
You may select filters based on Field Content or Record ID. You may also select None to indicate that no filter is set for the highlighted data type.
A filter based on Field Content evaluates data within a record to determine if the field meets the specified condition. When a field meets the filter condition, the record is synchronised.
A filter based on a Record ID allows you to select which individual records are to be synchronised. This feature is useful when you want to specify exact records to synchronise. For example, if you have personal contacts and business contacts in your Contacts list and you only want to synchronise the business contacts, using Record ID, you would select only the business contacts.
The Filter Description section displays the filter conditions that have been defined for the Selected data type. Rather complex filters can be defined, and each filter condition can be modified using this dialogue section. You can click on the links to modify or remove the filter conditions.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com



Data Sources:
To change the data source, select the item you want to change from the list and then click Change. If the translator does not support a change of data source, the Change button will be disabled.

If the translator supports the change, the Change button is enabled and this allows you to select a data source that you want the translator to work with. For example, if you have two Contacts folders, you can specify which folder is to be used as the contact source of data for the translator.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

3.14| how to upgrade the Firmware of your IsatPhone

3.14.1 installing the firmware upgrade tool

PLEASE ALWAYS DOWNLOAD Latest Firmware upgrade Tool from website when you upgrade your phone!

From time to time, it may be necessary to upgrade your phone in order to improve its functionality and operation. You will be notified by Inmarsat and/or your service provider when a firmware upgrade is required.

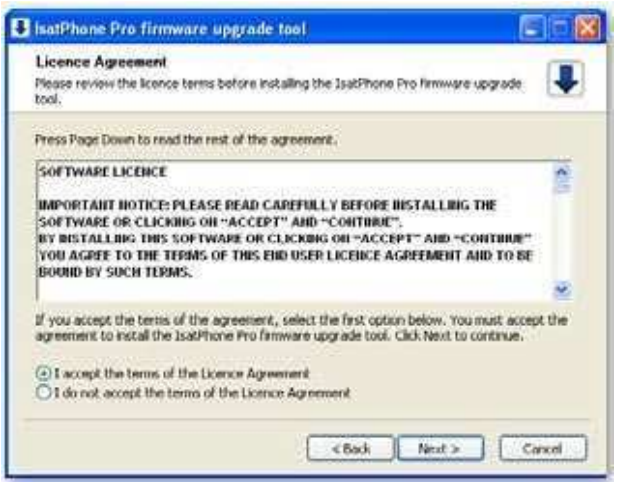
Please note that you need to install the USB drivers before installing the firmware upgrade tool. The USB drivers and the guide, 'How to install USB drivers' are included on your CD.

To install the firmware upgrade tool on your PC, perform the following procedure:

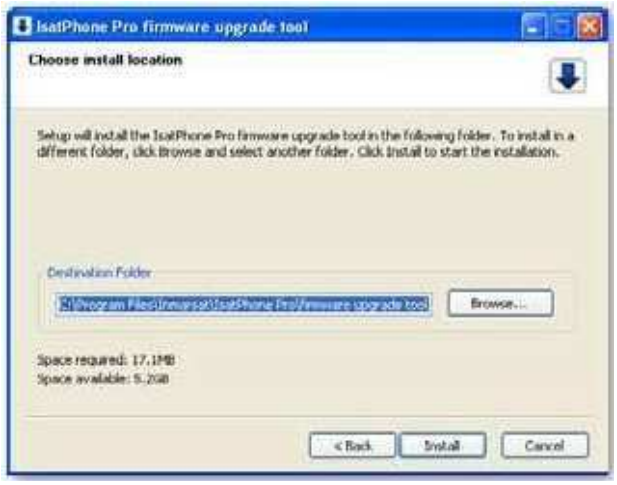
Select software > firmware upgrade tool
from the CD.
The IsatPhone Pro firmware upgrade tool
setup wizard appears.

Click Next.

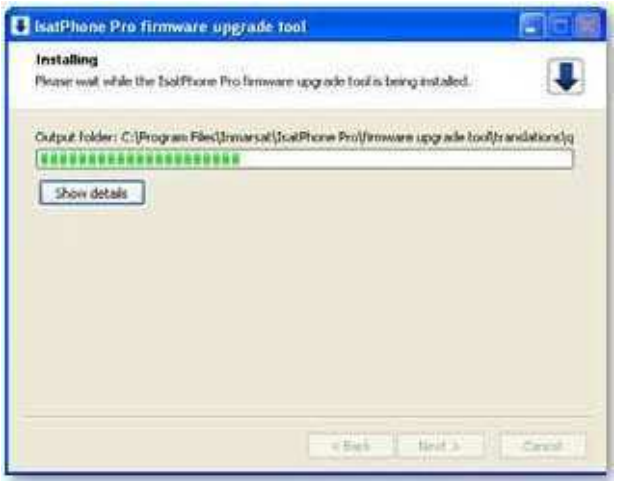
GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com



Read and select I accept the terms of the
Licence Agreement and click Next.



Click Install to begin the installation process.
Note: You can click Browse… to change the installation folder location.



Click Next after the installation process is complete.
Note: You can click Show details to display the installation details.

Click Finish.
The setup is complete.

Note: If Run the application is selected, the tool is launched once the setup is complete.

3.14.2 upgrading your IsatPhone

The firmware upgrade will be successful with or without the SIM inserted in your phone.
Upgrades can be forward- and backward-compatible and can be loaded non-consecutively, eg. from v1.0 to v3.0 except for Patches that must be forward- consecutively eg. from v3.0.2to v3.0.3
Please READ CAREFULLY Upgrading Instructions, if instructions are not attached or if you are not sure about what to do, always contact Geoborders Customer Care at the address support@geoborders.com.
Your personalised settings, for example PINs, contacts, organiser etc are unaffected by an upgrade. However, the contact synchronisation tool is available if you wish to create a backup of your contacts.
During an upgrade, your phone is powered from the USB connection. However, a minimum battery charge level is required to power on and to begin the upgrade.
If the upgrade is interrupted, your phone remains in upgrade mode and the upgrade should be restarted. Your phone will remain in upgrade mode until the upgrade has been successfully implemented.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Note: Before starting the firmware upgrade
tool, ensure that your phone is not connected
to your PC.
Select Start > Programs > IsatPhone Pro >
firmware upgrade tool > firmware upgrade tool.

Browse and select the .fpk file (upgrade image file)
and click Next.

If the file is not valid, for example an incorrect file has been selected or your phone is connected to your PC, an error message will appear.

Connect your IsatPhone to your PC with the
supplied USB cable. If your phone is not
switched on, switch it on now.
Note: When your phone is connected to your PC, the Start upgrade button is enabled, IsatPhone is connected and Ready to upgrade is displayed in the status field.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Click Start upgrade to begin the IsatPhone
firmware upgrade.
If your phone is disconnected or an error has
occurred during the upgrade, an error message is displayed. Correct and repeat the upgrade until successful.

On 100% completion of upgrade, Device upgraded successfully is displayed in the status field. Your phone is now successfully upgraded.
Click Finish to close the application. Your phone will automatically restart and enter the charging mode as the USB is still connected.
Remove the USB cable from your IsatPhone.

Your phone is ready to use.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

4| Frequently asked questions about IsatPhone Pro.

What coverage is available for the IsatPhone Pro?
The IsatPhone Pro will operate on a global basis over the three Inmarsat-4 satellites.

Who is the IsatPhone Pro for?
The IsatPhone Pro is primarily designed for users in the government, media, aid, oil and gas, mining and construction sectors.

What features does the IsatPhone Pro have?
At launch, the phone will support: Satellite telephony (including Bluetooth for handsfree use) Voicemail Text and email messaging GPS location data (view position and text)

How is the sim card inserted into the IsatPhone Pro?
Remove the battery cover by using a coin to turn the screw slot on the back of the ISAT phone, until it is vertical. If the battery is in place, lift it out. Slide the catch down on the SIM holder and flip it outwards. Make sure the angled corner of your SIM card is on your left and slide it into the holder. Flip the holder back into place and slide the catch back up. Insert the battery, replace the cover and turn the screw slot until it is horizontal.

How is the IsatPhone Pro switched on and off?
Hold down the red key which is found on the top right of the main keypad, until the screen lights up. The first time you use your phone, use the navigation keys to select your language and set the time zone. To switch off, hold down the red key until the screen shuts down.

How does the IsatPhone Pro connect to the Inmarsat network?
Stand outside with a clear view of the sky with the phone antenna pointing upwards. There must be a clear line of sight between the phone's antenna and the satellite. The more sky you can see the stronger the signal should be from the satellite. If open sky makes up about 70% of your view when you look up, then the signal should be strong. Searching satellite will appear on the screen. The top left of the screen will display Inmarsat when your phone is connected to the satellite. The signal bars indicate the signal strength. At least two signal bars are required to make and receive calls.

How does the IsatPhone Pro obtain a GPS fix?
Before a call can be made, the phone needs a GPS fix so it can be located by the satellite. This happens automatically but if a new GPS fix is needed, the GPS fix icon will be displayed on the screen. The phone should be kept in the open with a clear view of the sky until the icon on the screen disappears. Once this is done the phone is now ready to register with the network.

How to use FREE GOOGLE MAP tracking?
Register your phone to Geoborders Website and simply send an email message from the phone to tracking@geoborders.com you will see your position on the website and depending of your settings the website can forward your position to some email addresses and to Facebook and Twitter.

Can a GPS fix be obtained manually?
If the phone continues to show the GPS fix required icon (which means that a new GPS fix is needed) select Menu > GPS position. The new GPS fix is displayed. When this screen is open, the phone will attempt to refresh the GPS fix every 30 seconds.

Where is the IMSI (sim card number) found on the IsatPhone Pro?
The IMSI number is displayed under Menu > Settings > About.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Where is the Firmware version found on the IsatPhone Pro?
The Firmware version is displayed under Menu > Settings > About.

Where is the IMEI number found on the IsatPhone Pro?
The IMEI number is displayed under Menu > Settings > About.

How is an incoming call answered on the IsatPhone Pro?
Firstly the antenna has to be deployed. When the phone rings, press the green button to answer the incoming call.

How is an ongoing call terminated on the IsatPhone Pro?
Press the red button to end/terminate a call.

How is an outgoing call made on the IsatPhone Pro?
To make a call enter the full international number by dialling +,then the country code, area code (without the leading 0), telephone number and then press the green key, eg. +44 1621 123456.

How is the redial feature used on the IsatPhone Pro?
If you press the green button you can see a list of the previous numbers which you have dialled. Cycle through the numbers with the cursor keys, and when you reach the one you want to call press the green button again to call it.

How is an incoming call declined before it is answered on the IsatPhone Pro?
When there is a incoming call and the phone is ringing you can press the red button to decline it. The details of the calling party will now be stored in the call register, under missed calls.

How is the voicemail feature accessed on the IsatPhone Pro?
To retrieve and listen to voicemails press and hold down the 1 key, or dial 57. This will then automatically dial your voicemail inbox. Alternatively you can dial the voicemail box directly on +870 772 001 899 and press the green key to dial.

How is the IsatPhone Pro's battery charged?
Plug the charger into the power source. Then connect the mini USB connector from the plug into the base of the phone. Leave to charge until battery is full (it's important to fully charge when first purchased).

How is the keypad locked on the IsatPhone Pro?
You can lock the keypad by pressing the mains key in the centre of the phone followed by the * key. Only the green and red buttons will be active now

Will data services be available on the IsatPhone Pro?
A circuit-switched data service at 2.4kbps is expected to be available on the IsatPhone Pro during Quarter one 2011. Users will be able to upgrade their firmware on the handset to use this.

Will the IsatPhone Pro be blocked for pre-pay use in the United States?
No. Isatphone both prepaid and postpaid work in USA

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5| Best Practice Summary for: BGAN, FB and SWB.

5.1| Remote Terminal Installation

5.1.1 Pre-Installation Planning

A Pre-Installation Planning is essential because of Different Terminal Features and possible Configurations.
All of the Inmarsat terminals provide different services for the particular class or type of terminal that you have purchased or plan to purchase. However, equipment from different manufacturers may differ slightly in respect of features, configurations and physical interfaces.
Before you take delivery of your Inmarsat terminal make sure that it has the features that you require to support the peripheral devices, such as for example, routers, hubs, handsets, PABX's, and applications that you wish to connect to your terminal.

5.1.2 Overview

Inmarsat is a robust communications system that will provide reliable communications across the globe in all weather conditions. However, in order to get the best performance out of your system it is essential that the equipment, both above decks and below decks, is correctly installed. A well thought out and designed installation will ensure consistently high data throughputs and minimise, or even eliminate, outages due to shadowing.
This section provides guidance on all aspects of the installation of the terminal on the vessel together with some best practice recommendations.

5.1.3 Equipment location

Ideally the antenna should be installed on the highest point of the vessel with a clear view of the sky in all directions and all possible steps should be taken to achieve this objective.
If it is not possible to mount the antenna with an unrestricted view of the sky then the antenna should be positioned so as to ensure minimum shadowing from the vessel superstructure such as funnels, radar etc. Such positioning should take into account the typical shipping routes used by the vessel and the azimuth and elevation required for communication under way with the appropriate satellite.
In circumstances when shadowing might occur it is useful (and good practice) to create a "shadow area" chart for use on the bridge showing at which azimuth shadowing may occur for each of the Inmarsat satellites to be used. An example of a shadow area chart is given below in Figure 9 which shows that, for this particular installation, shadowing will occur at azimuths of 120° - 122° and 187° - 196°.
If shadowing is a major problem then consideration should be given to the installation of two antennas – one either side of the superstructure – and the provision of a selector switch (manual or automatic) to select the antenna with the clearest view of the satellite.

NOTE: Ensure that the antenna is fitted on the antenna pedestal pointing forwards as indicated by the forward arrow on the base of the antenna.

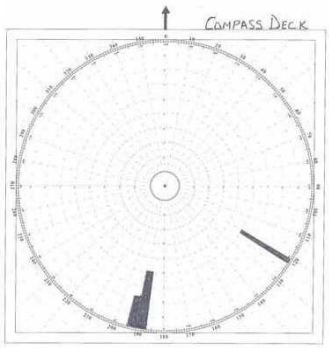


Figure: Example Shadow Area Chart

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.1.4 Hotworks

Hotworks can usually be carried out by the crew in advance of the installation of the antenna itself. Such works will include fabrication and mounting of the antenna pedestal (taking into account the shadowing factors described above in Section 3.2.1) and, possibly, through-deck penetrations for the antenna cabling.
The completion of this preparatory work by the crew will ensure that the work is carried out in accordance with the shipping company practices and that the subsequent equipment installation is carried out in the shortest possible time.

5.1.5 Antenna Cabling

The Inmarsat antenna uses a single cable which carries both the power for the antenna stabilisation system and the RF signal. Maximum distance between the antenna unit and the Below Decks Equipment (BDE) is determined by the type of cable used and will be specified in the manufacturers installation instructions. Cable runs can be of the order of 25 - 100 metres depending on the antenna cable used. Some typical cable runs are shown below in Table 4.

Cable Type	L (min)	L (max)
RG-223	7 m	25 m
G214 - FRNC	12 m	50 m
S10162B11	30 m	100 m
RG ½" 50	45 m	100 m

Table: Typical Antenna-BDE Cable Runs

This table is provided for guidance only – you should consult the manufacturers installation manual for specific guidance on the actual cable type and length for use with your particular terminal.

5.1.6 IP Network Cabling, Wi-Fi and Voice/Fax/Data Port Locations

going to be installed and the location of the devices (telephone handsets, fax machine, routers, PCs etc) that are going to be connected to it.
You should also note that, if you are installing a wireless LAN to work with your Inmarsat system, the signal from a wireless LAN will not penetrate the steel bulkheads on a modern ship. If wireless connectivity is desired, provision needs to be made for the installation of a wireless repeater in each cabin or accommodation area.
Additionally, if required, the use of high quality Cat 5 or Cat 6 cabling is recommended, ensuring that the cable has appropriate flexibility and shielding.

5.1.7 Power

Inmarsat has no special power requirements beyond what is normally available on a ship. Power is delivered in a single cable together with the RF from the BDE to the antenna.
Typical BDE power requirements are 12-32 Vdc, 150 watts. For specific power requirements please consult the manufacturers installation manual for your particular terminal.
Depending on how "clean" the power supply on the vessel is, consideration could be given to the use of power conditioning units for use with the Inmarsat BDE and associated network equipment and peripherals devices.

5.1.8 Fast Installation without downtime

The Inmarsat antenna is significantly lighter than previous Inmarsat antenna units and can be lifted and installed by at most two persons (unlike previous Inmarsat systems that required the use of the crane alongside).
As such, if all of the preparatory work as described in this Section 3.2 has been effectively carried out the physical installation of the system should only take a few hours and not require any time beyond that normally spent in port.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.2| HQ Installation

5.2.1 Connecting to Geoborders – the "Last Mile"

Inmarsat manages the Quality of Service (QoS) within the Inmarsat network, QoS being defined by various parameters including bit-rate, latency, jitter and packet loss. When a Inmarsat data connection is opened, the QoS for the connection is negotiated between the Inmarsat terminal and the Inmarsat Core Network and is determined by the type of data connection requested – Standard IP or Streaming IP.

To ensure that a consistent QoS exists for the full end-to-end connection the quality and speed of the connection between your Local Geoborders Branch or Service Provider and your corporate network, often referred to as the "last mile", needs to be commensurate with the type of Inmarsat service and associated application(s) that you wish to use.

Last-mile connectivity for a Standard IP connection can be simply and effectively implemented using Internet-based solutions. However, if an Internet-based solution is used for last-mile implementation there is no guaranteed QoS.

A Streaming IP connection requires a more demanding QoS than a Standard IP
connection and QoS is particularly important for UDP-based applications such as live video and audio streaming. In such instances Inmarsat recommends that guaranteed QoS last-mile routing arrangements such as a dedicated connection are implemented.

Section 5.5 below, entitled Selecting an IP connection type, describes the characteristics of the two Inmarsat connection types – Standard IP and Streaming IP – and provides guidance on selecting the most appropriate connection type for different applications. Once you have decided on the most appropriate Inmarsat connection for your applications you should then choose the appropriate last-mile interconnect.

Your Inmarsat Service Provider can provide details of available interconnect options and assist in the selection of the most suitable last-mile connection for your application(s).

5.2.2 Internet-based Last-Mile solutions for use with a Standard IP connection

Most typical office applications such as email, Internet browsing and FTP and numerous maritime applications such as electronic charts and weather updates are best suited to Standard IP combined with an Internet-based last-mile implementation as shown below in Figure 10.

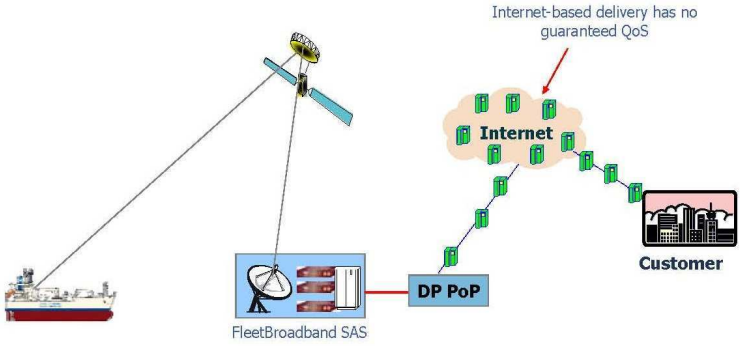


Figure: Internet-based Last Mile Implementation

However, if Internet connectivity is highly contended and the overall connection quality is impaired it may be worth considering the use of a dedicated circuit for last-mile connectivity, as described below in Section 4.3, for use with your Standard IP connection.

From the shore-side access to the Internet by the corporate/office network could be by any one of several means such as:

- Dial-up
- ADSL/DSL
- wireless
- cable
- VSAT (shared or dedicated)

5.2.3 Guaranteed Last-Mile solutions for use with a Streaming IP connection

A Streaming IP channel is similar to a circuit-switched channel in that both are charged by time and both guarantee a certain QoS to the terminal. Streaming IP is optimised for use with audio and video applications such as Windows Media and QuickTime and synchronisation of enterprise solutions such as Oracle and SAP.

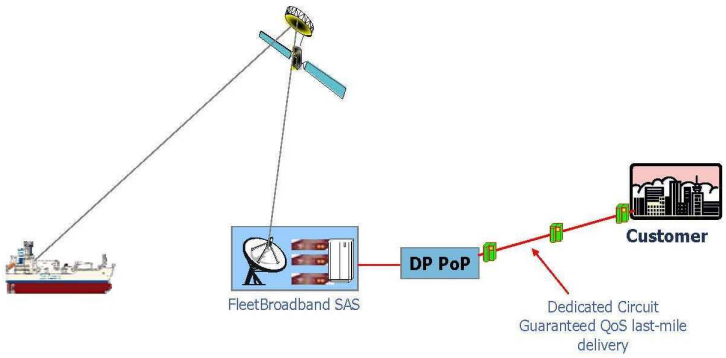


Figure: Dedicated Circuit Guaranteed QoS Last Mile Implementation

The following dedicated connection types would be suitable for use with a Streaming IP channel

- Basic and Primary Rate ISDN
- Leased line
- Internet-based MPLS
- Diffserv

5.2.4 Local Geoborders Branch (DP) Infrastructure Considerations

Have you selected your Inmarsat Local Geoborders Branch yet? Whether you have or you haven't you need to ensure that your DP has the infrastructure to support the applications and configurations that you wish to implement in your network such as:

Customers to have the	DP with Shared infrastructure	DP with Own Infrastructure
Ability to do IP Streaming End-to-end	No ?	Yes
User customised "Last mile" connections & End-to-end QOS Streaming: ➢ Bonded ISDN ➢ Leased connections ➢ MPLS / Diffserv based IP QOS connections ➢ Worldwide / Regional meet-me Points-of-presence (POP)	No ?	Yes
Customised IP Addressing Open, Closed Network connectivity Radius server for Own IP allocation & Authentication?	Yes No No	Yes for all Public, Private, Dynamic & Static
Firewall Customisation	No	Yes
Flexibility of Own APN & User ID & Logon facility	Yes but....	Yes
"Real-time" access to User Accounts/SIM info	Yes	Yes

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Note: In order to take full advantage of the guaranteed QoS provided by the Streaming IP service the Streaming IP channel must be used in conjunction with a last-mile connection with a similar guaranteed QoS.

Some of the features you may need from your Local Geoborders Branch are:

1. World-wide network of local PoP's
2. Infrastructure QoS considerations such as:
    - bandwidth, Traceroute points or TTL values
    - latency and jitter
3. Flexibility/Choice of VAS Services
    - firewall and/or security solutions
    - proprietary or optimised data communications solutions
    - billing systems access
4. Integration/Optimisation/Middleware/Gateway Support
5. Speed and personalisation of support
6. Consultancy and support (SatCom, IT and IP)
7. Integration and custom infrastructure access
    - IP Addressing
    - SMTP
    - web storage facilities/portal access
    - market-specific custom applications
    - unified messaging features
8. Acceleration middleware
9. Deployment and training

5.3| VPN Implementation

Virtual Private Networks (VPN's) are an integral component of most corporate networks and it would be only natural that one would wish to extend the reach of the corporate VPN offshore using the data networking capabilities of Inmarsat. Such an approach would be quite workable and most commercially available VPN implementations will operate seamlessly over Inmarsat.
A large data overhead (20-40%) is inherent in the implementation of a VPN but for a conventional terrestrial broadband network connection such overhead has little or no
impact on either cost or performance. However, when using a mobile satellite-based network connection this overhead can have an adverse effect on both cost and performance resulting in higher costs and reduced bandwidth.

Consideration should therefore be given to provision of a leased or dedicated connection (see Section 4.3 above) between the shore-based corporate network and the DP and connecting remote offshore users to the shore-based corporate network by assigning a static private IP address to each vessel on the network.
Such a configuration will remove the requirement for a VPN client on the vessel and hence eliminate the overhead associated with the use of the VPN, while maintaining the integrity and security of the entire corporate network.

VPN clients tested by Inmarsat over the Inmarsat network include those from:

- Checkpoint NG
- Cisco
- Netscreen
- Nortel
- PPTP

Inmarsat has also successfully operated secure Internet protocols such as IPSEC, L2TP, SSL and HTTPS across the Inmarsat network.

5.4| Corporate Intranet Design Considerations

You should consider having a "light" version of your corporate Intranet for use by remote users such as Inmarsat users. Guidelines for the design of such a web site can be found at http://www.thedigitalship.com/webguide/technicalinfo.html

5.5| Implementation Notes for Corporate Enterprise Systems

Corporate enterprise solutions such as Oracle, SAP, CRM and ERP are becoming increasingly widespread. Such systems can be characterised as:

- "heavy" data-intensive systems
- designed for megabit/gigabit networks
- using very chatty protocols

As such they are not very "light" and therefore not usually "mobile friendly".
If such a system is to be used in conjunction with the Inmarsat network it must be optimised (usually by the supplier of the product) to operate effectively in wireless/mobile conditions in order to reduce overheads, support high latency and implement effective crash recovery.
Other enterprise solutions optimised for the maritime environment are also available from specialist maritime providers such as:-

- SpecTec www.spectec.net
- Danaos www.danaos.com
- Horizon Mobile Communications www.horizon-mobile.com

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.6| Vessel Network Considerations

5.6.1 Typical remote or Vessel Communications Network

Inmarsat is a flexible and versatile communications system capable of providing a cost-effective communications platform for the wide range of devices and applications that are to be found on a modern ship today. A typical vessel configuration might well look like the system shown below in Figure 12

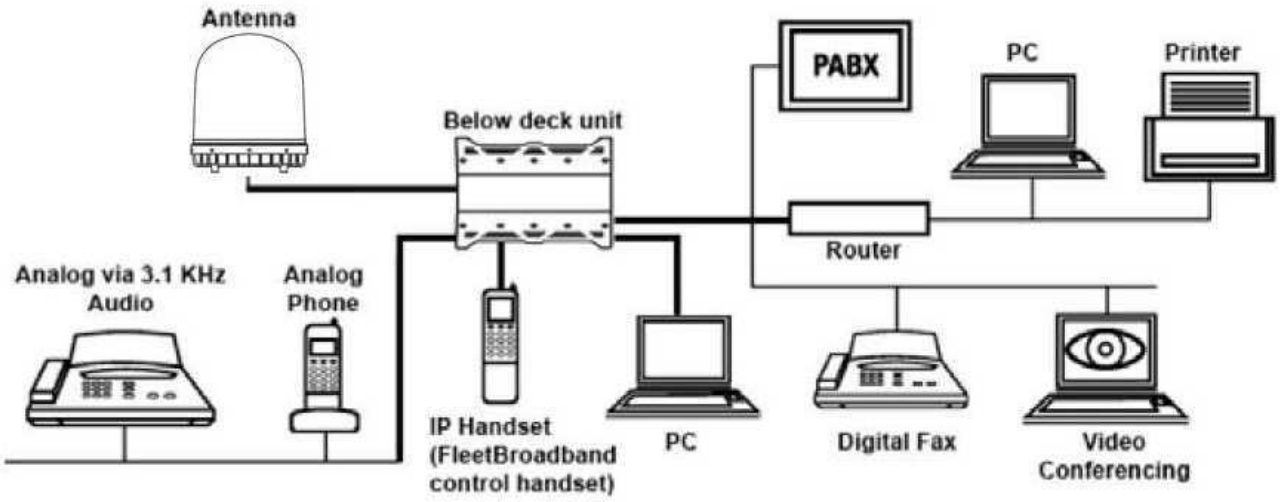


Figure: Typical Vessel Communications Network

6.2 Integration with existing communications infrastructure

Consider what existing communications equipment and peripherals you wish to retain on board and why? Some examples of applications or peripherals that you may wish or need to connect to your Inmarsat terminal are:

- Handsets: Analogue, Cordless, DECT, ISDN
- Wireless Wi-Fi network
- VoIP Peripherals: USB, Wi-Fi Phones
- Audio: Conference systems
- LAN/WAN Devices: Routers, Hubs, Switches, Wireless Access Points
- IP/Network Cameras: Remote Surveillance
- Off-the-Shelf Video:- Scotty-motion Media, Polycomm, Sony IP
- Legacy ISDN devices

How do you propose to integrate existing communications equipment with your Inmarsat and how will you determine which communications system to use and in what circumstances?
Consider an optimal cost routing system or automatic or manual switch. Some third-party routing solutions are available from your DP or SP or from specialist providers such as:

- Becker Marine UMC
- Dualog
- Livewire – Selector Switch
- Virtek

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.6.3 Integration of other subsystems on board

Nowadays many onboard systems are data network-enabled and can be connected to the onboard LAN. Such connectivity when used in conjunction with Inmarsat will permit remote monitoring of onboard systems such as:

- Water Filtration Systems
- Refrigeration Systems
- Engine Telemetry Sensors
- Condition-based Sensors/systems
- Preventative/Predictive Maintenance Systems
- Weather Sensors – Receive/Sending
- Container Loading/Unloading Monitoring Sensors
- Container/Cargo Monitoring or Tracking Devices

5.6.4 Ethernet options/sub-networks

Consideration should be given to configuring the onboard Ethernet wiring implementations into sub-networks such as, for example, a bridge network, engine network, crew network as shown below in Figure 13, in conjunction with a suitable combination of servers and third-party solutions such as those mentioned above in Section 5.2 and 5.3.
Such an approach will enable the differentiation of the various networks according to importance and hence prioritisation, bandwidth allocation, network-specific optimum/least-cost routing etc.

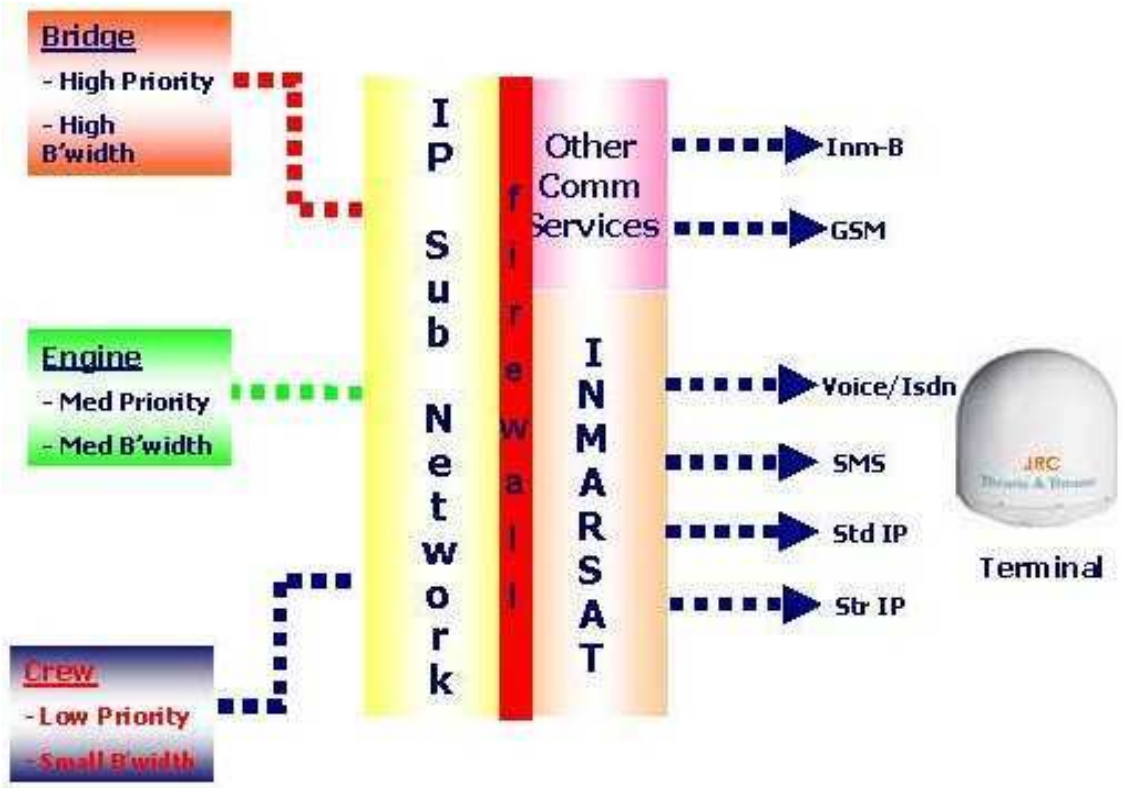


Figure: Example of Vessel Sub-Network Implementation

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.6.5 Selecting an IP connection type

Inmarsat supports two types of IP data connection designed to meet the full range of your IP data requirements. They are:

- Standard IP
- Streaming IP

Two types of Streaming IP connection can be set up – basic Streaming IP and dedicated Streaming IP.
Basic Streaming IP is a single connection through which all traffic is routed from the terminal to the destination. If multiple connections with independent routing are required then dedicated Streaming IP should be selected and set up.
Refer to the User Guide for your Inmarsat terminal for information on opening and closing an IP data connection.

5.6.5.1 Standard IP

The Standard IP channel utilises the network capacity that is not allocated for streaming channels. This capacity is shared between all terminals that are using the network, and so the actual performance varies depending upon how many terminals are connected, the location of the terminals and the number of channels in your particular spot-beam.
A Standard IP data connection is pre-configured on the Inmarsat terminal and opens automatically when the terminal is connected to the Inmarsat network. It offers data rates of up to 432kbps (depending on the terminal) shared with other users on a "best effort" basis. Inmarsat monitors the usage in each spot beam and as usage increases extra satellite resources are dynamically assigned to individual spot beams in order to meet demand.
Standard IP is best suited to most typical office applications such as Internet browsing, e-mail, FTP and also numerous maritime applications such as electronic charts, weather updates, engine monitoring and many more. This is the type of connection that will be used for most of the time and for most applications.
Refer to your Inmarsat Service Provider for details on how you are charged for a Standard IP connection.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.6.5.2 Streaming IP

A Streaming IP channel should be selected when a guaranteed Quality of Service is required for your applications (e.g. real-time video, un-optimised enterprise solutions, database synchronisation, etc). A streaming channel is similar to a circuit-switched channel, in that both are charged by time and both guarantee a certain throughput or bandwidth to the terminal.

A streaming channel is set-up between the terminal and the streaming end-point, which may include the connection between your DP and your corporate network – the "last-mile". Note that the data must pass through a number of routers and possibly a firewall between the terminal and your corporate servers.

To ensure guaranteed end-to-end Quality of Service Inmarsat recommends the use of a managed "last-mile" such as a leased line or ISDN backhaul - for availability see
your Local Geoborders Branch or Service Provider.

Note:
There may be a minimum charge when a Standard IP data connection is open, and data may be transferred across the connection even if you are not actively using an application (for example your computer may be receiving automatic updates - see Section 9.4 below entitled Automatic Updates).

Note: If the network is unable to provide sufficient resource for the requested streaming channel, it either provides a lower capacity streaming channel, uses the standard channel or refuses access, depending on your Inmarsat LaunchPad settings for that connection

It is possible to configure Streaming IP data connections on the Inmarsat and open two or more Streaming IP connections in addition to the Standard IP connection – see next section for further information on setting up multiple dedicated Streaming IP connections.

Streaming connections are available at the following data rates (depending upon terminal type):

- 32kbps streaming
- 64kbps streaming
- 128kbps streaming
- 256kbps streaming

Streaming IP is optimised for use with UDP applications, such as video and audio.

The Streaming IP Quality of Service (QoS) is consistent and guaranteed. However, the observed throughput may be slower than the rate selected because of application overheads such as the packet header size etc. In addition, any interconnect with terrestrial networks may impact the throughput.

Refer to your Inmarsat Service Provider for details on how you are charged for a Streaming IP connection.

Note: Ensure that end-to-end QoS is supported for the required Streaming IP data rate. This is discussed further in Section 4.3 above, entitled Guaranteed Last-Mile solutions for use with a Streaming IP connection.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.6.5.3 Dedicated Streaming IP

A dedicated Streaming IP connection enables the creation of multiple connections – each of which can be "dedicated" to selected individual applications that need to run simultaneously. By using port forwarding (see Section 7.4 below) it is possible to "route" these dedicated connections to multiple devices on the network as well as multiple physical locations.
In the example shown in the diagram below a Standard IP connection is open and is being shared by terminal users for IP data applications such as Internet and e-mail services. In addition, two dedicated Streaming IP sessions are open - the first, at 32kbps, is being used exclusively for an audio streaming application and the second, at 128kbps, is being used exclusively for a video streaming application.
You must assign a dedicated Streaming IP connection to a specific application such as Windows Media, real-time video, un-optimised enterprise solution, database synchronisation, etc.

The maximum number of dedicated Streaming IP connections depends on the terminal's capacity for supporting Streaming IP e.g. for an FB500 model 1 x 256, 2 x 128, 4 x 64 or 8 x 32 kbps connections can be simultaneously set up.

A dedicated Streaming IP connection uses the routing information of the Standard IP connection. Therefore, a Standard IP connection must be open before a dedicated Streaming IP connection can be set up. (A Standard IP connection is opened automatically when a Inmarsat terminal is connected to the network). Note that one of the pre-configured Streaming IP connections can be opened as an alternative to the Standard IP connection.
In order to enable the Inmarsat terminal and Inmarsat network to work together to "route" these multiple connections successfully a Traffic Flow Template (TFT), also called an Application Template, is used. In the Inmarsat terminal the TFT is associated exclusively with a secondary PDP context, i.e. with a dedicated Streaming IP connection. See Section 5.8 below for more information on Traffic Flow Templates.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.6.5.4 Which IP connection should I use?

You can maximise throughput and performance and minimise your traffic costs by selecting the Inmarsat IP connection type best suited to the application being used. In considering which is the best connection to use for a particular application one needs to take into account not only the Quality of Service (throughput and performance) required but also the nature of the commercial agreement with your SP or DP and cost-factors including:

- data volume
- session duration
- fixed charge per connection
- minimum charge per session
- subscription charges

Table 5 below, entitled Which IP Connection Should I Use?, shows the most common applications used over Inmarsat, the recommended IP connection type and further details of how to effectively use the connection.
The table is for general guidance only and a more specific analysis of the most appropriate connection type for a particular application should always be carried out using the guidelines contained in this Section 5.5, entitled Selecting an IP connection type, and Section 9 below, entitled Communication Cost Management.

Application type	IP Connection type	Further details
Email	Standard IP	Standard IP is ideal for sending/receiving emails
Internet browsing	Standard IP	Standard IP is best suited for Internet browsing
VPN	Standard IP	Standard IP is suitable for VPN connections
FTP	Standard IP	Inmarsat Broadband is optimised for sending and receiving files using FTP over Standard IP
Voice	AMBE 2 (4kbps) / Standard IP	Voice calls can be made over the voice service
VoIP	32 kbps Streaming IP	Voice AMBE 2 calling should be used whenever possible
Fax	Voice 3.1KHz / ISDN / Standard IP	Fax can be sent/received using either the 3.1kHz voice service (Group 3 fax), ISDN (Group 4 Fax) or fax over IP.
Videoconferencing / Teleconferencing.	64/128/256 kbps Streaming IP (Standard IP offers no guarantee of quality)	Most videoconference equipment that can use IP data is suitable for use over Inmarsat.
Live Broadcast	256 kbps Streaming IP	Inmarsat 256 kbps service allows the delivery of cutting edge live video from almost anywhere in the world.
GSM	32 kbps Streaming IP or lower (Standard IP offers no guarantee of quality)	This solution allows passengers to use their own devices to make phone calls.
Secure communications	Depends on application	Inmarsat can be used to deliver secure communications including STU-III, STE, messaging, voice, fax, video and data.
Remote data delivery	Standard IP	FleetBroadband can be deployed as an unmanned communication point to deliver results from monitoring sensors to video surveillance suites.

Table: Which IP Connection Should I Use?

Tip: If you are unsure what type of connection to use for a particular application try first with Standard IP.

5.7| LaunchPad, Web Interface and AT commands

5.7.1 LaunchPad

LaunchPad, shown below in Figure 14, is the interface and control application developed by Inmarsat for use with its range of broadband terminals including Inmarsat. LaunchPad provides the following features:

- Familiar and simple access for the full range of Inmarsat terminals.
- Easy to use, train and support – same interface is used for all manufacturers and model types
- Provides standardised diagnostic and status display for all manufacturers and model types
- Provides SMS for multiple users
- Clear status display
- Incorporates TCP PEP

Figure: Inmarsat LaunchPad Home Screen

5.7.2 Web Interface

Some manufacturers provide a web-based interface for the configuration and control of the Inmarsat terminal such as that shown in Figure 15 below, entitled Thrane & Thrane Inmarsat 500 Web-based Interface

Figure: Thrane & Thrane Inmarsat 500 Web-based Interface

5.7.3 AT Commands

Inmarsat terminals can also be configured and controlled using AT commands via Telnet. AT commands are executed from a DOS command prompt and sessions are initiated using the telnet command to connect to the terminal. DHPC settings for each of the currently available terminals are shown below in Table 6

Terminal Manufacturer	Telnet Interface and Ports
Thrane	192.168.0.1 port 5454
JRC	192.168.128.100 port 1829

Table: AT Command Interface

Some typical Inmarsat AT commands are shown in Table 7 below.

AT Command String	Command
ATE1	Switch on Local Echo of text
AT+CGMR	Check terminal for firmware version
AT_IGPS?	Determine if GPS has been set
AT+CGDCONT?	Check the IP connection parameters and Public IP address returned
AT+CGDCONT=11,"IP", "FleetBroadband.inmarsat.com"	Set the IP connection parameters
AT+CGACT=1,11	Start the IP connection setup above
AT+CGPADDR=11	Check what your Public IP Address is?
AT+CGEQREQ=1,1,256,256,256,256,1500,E30, E40	Set the QoS parameters for a Streaming IP connection

Table: Typical Inmarsat AT Commands

5.8| TCP/IP and UDP/IP

UDP/IP over the Inmarsat network. It provides information on the performance of each protocol on a Streaming IP data connection and recommends how to configure your data connections and applications to maximise performance.

5.8.1 About TCP/IP

TCP (Transmission Control Protocol) is used for normal Internet traffic and applications such as web-browsers, FTP and so on, where data delivery must be guaranteed. TCP/IP requires packet re-transmission, that is the re-sending of dropped or lost packets to ensure that all data is transmitted.

Packet re-transmission is a standard feature on all networks running applications over TCP/IP. One result of this is the reduction in perceived IP throughput rates as the protocol waits for the re-transmission of dropped or lost packets. In addition, TCP/IP applications throttle their rate of packet transmission based on the capacity of the link. For these reasons, TCP is best suited to an IP connection optimised for packet re-transmission, and ideally with as large a capacity possible.

Recommendation: Inmarsat recommends the use of a Standard IP connection, with data rates of up to 432kbps, for TCP-based applications such as email and FTP.

The characteristics of TCP/IP traffic are not as well suited to the Streaming IP connections available on the Inmarsat Network. Each Streaming IP connection is a dedicated connection designed for a single IP packet stream at a fixed rate of throughput (up to 256kbps). A Streaming IP connection is better suited to time-critical applications where rapid transmission of data is more important than dropped or lost packets. Such applications are also better suited to the UDP protocol.

Should you decide to use TCP/IP applications over an IP Streaming data connection, you may experience the following:

- In the from-vessel direction, a typical 10-15% reduction in throughput due to network signalling and application overheads, plus a further 10-15% reduction based on TCP packet retransmission. The achieved IP throughput could therefore be up to 30% less than the desired streaming rate.
- In the to-vessel direction, the affect on performance could be the same as the from-vessel direction. In addition, there is the risk of further dropped packets should data burst at a rate higher than the capacity of the connection. In this scenario, packets are repeatedly lost and re-transmitted until the Inmarsat link has the capacity to forward them to their destination. This may cause a further 10% reduction in throughput.

5.8.2 About UDP/IP

UDP (User Datagram Protocol) is used for applications such as video streaming or audio streaming, where lost packets don't need to be retransmitted and speed takes precedence. Unlike TCP/IP, any dropped or lost packets are ignored and compensated for or replaced by the application. This application intelligence optimises transmission speed and is particularly effective on non-contended connections, such as Streaming IP connections on the Inmarsat network.

UDP applications throttle their transmission rate according to the capacity of the
connection but they do not retransmit packets. The achieved data rate is therefore much closer to the desired connection rate.

Recommendation: Inmarsat recommends Streaming IP connections for live video and audio streaming applications which are better suited to the UDP protocol.

5.8.3 Traffic Flow Template (TFT)

connections are required. A Traffic Flow Template (TFT) is a series of up to eight filters that allows traffic that matches the filters to be routed on a particular PDP context and given a different QoS to traffic on other PDP contexts. When incoming data arrives at the terminal a packet classifier makes a PDP context selection based on the TFT and maps the incoming data packets to the correct PDP context with specified QoS attributes. In this way, multiple PDP contexts (called secondary PDP contexts) can be associated with the same PDP address as defined by the primary PDP context.

A number of TFT's are supplied with Inmarsat LaunchPad. Users can modify these for their own applications, for example videoconferencing or VoIP.

Please refer to the "Using TFT's on Inmarsat" guide available from the Inmarsat support website.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.8.4 Security Settings and Related Value Added Services

5.8.4.1 Firewall

It is strongly advised that a firewall is installed between the Inmarsat terminal and the vessel network to prevent unauthorised access to the vessel network. Some Local Geoborders Branches provide firewall solutions that are optimised for use with Inmarsat such as Trench from Stratos.

5.8.4.2 Proxy Server

A proxy server is a network device that stores information that is most often requested by network users in a cache on the network. Hence if a network user requests information which is already stored in the cache of a proxy server the server can deliver the files immediately thus enhancing the performance of the network and saving unnecessary communications costs.
An anonymous proxy server is able to mask an IP address from external network resources (e.g. web servers) which are accessed on the Internet. This prevents those resources from gathering information about your computer and hence significantly reduces the vulnerability of your computer and network to external security threats.

5.8.4.3 MAC address management/control

MAC is a mechanism to support access control and identification of computers on an IP network. MAC assigns a unique number to each network device called the MAC address. A MAC address is 48 bits long and is commonly written as a sequence of 12 hexadecimal digits which will be something like:
48-3F-0A-91-00-BC
When using MAC address access control on your wireless network, the wireless base station will check the MAC address of the connecting client and check to see if it is on a list of registered clients - if it is you get connected, if not you don't.
MAC address access control used to be useful but is really no longer a real option when it comes to wireless security. The problem arises as the MAC addresses are sent unencrypted and therefore can be picked up and read by a determined hacker.

5.8.4.4 DDNS (dynamic domain name server) updating

A Dynamic Domain Name Server is a network service that provides the capability for
a networked device, such as an IP router or computer system, to notify a Domain Name Server to change, in real time the active DNS configuration of its configured hostnames, addresses or other information stored in a DNS.

5.8.4.5 External Router

Consider adding an external router(s) for additional required features that are not integrated in the terminal. The following routers have all been used successfully with Inmarsat:

- Netgear
- D-Link
- Cisco
- US Robotics

5.8.4.6 DP Filtering

As well as changing the settings on your computer, you can ask your Service Provider or Local Geoborders Branch to filter some of the traffic before it reaches the Inmarsat terminal. This filtering takes place in the core network. Consult your Service Provider or Local Geoborders Branch for further information.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.9| Optimising IP settings

This section explains how to optimise IP to get the best possible performance and cost savings over Inmarsat. Any application using the TCP or UDP protocols invariably uses some standard TCP/IP services. These services can generate extra traffic over the network and should be configured to ensure that the data overhead, and associated cost, is kept to a minimum.
In addition to the standard Internet protocols, Inmarsat has also successfully operated secure Internet protocols such as IPSEC, L2TP, SSL and HTTPS across the Inmarsat network.

Tip: Make sure error correction is turned off for Streaming IP connections (it is switched off by default). Error correction settings cannot be changed for the Standard IP connection.

5.9.1 Satellite Latency and Jitter

Latency in the Inmarsat network comprises several factors as follows:

- physical distances involved ~ 500 ms (satellite-to-earth propagation delay)
- processing delay within the network infrastructure ~ 250 ms
- size, availability and prioritisation of appropriate time slots ~ 150 to 400ms

The total latency of the Inmarsat network is therefore in the range 900ms to 1150ms compared to the latency of a typical office LAN or ADSL connection which is of the order of 15-100ms. The absolute latency of the Inmarsat network is therefore not only a significant factor to be taken into account in itself but its variability, known as jitter, also becomes a significant factor that needs to be considered.
There are significant differences between jitter in a Standard IP connection and jitter in a Streaming IP connection – see Figure 16 below.
End to End Latency should therefore always be taken into account and particular attention should be paid to terrestrial networks employing VSAT or other satellite links that will introduce “double-hop” delays.

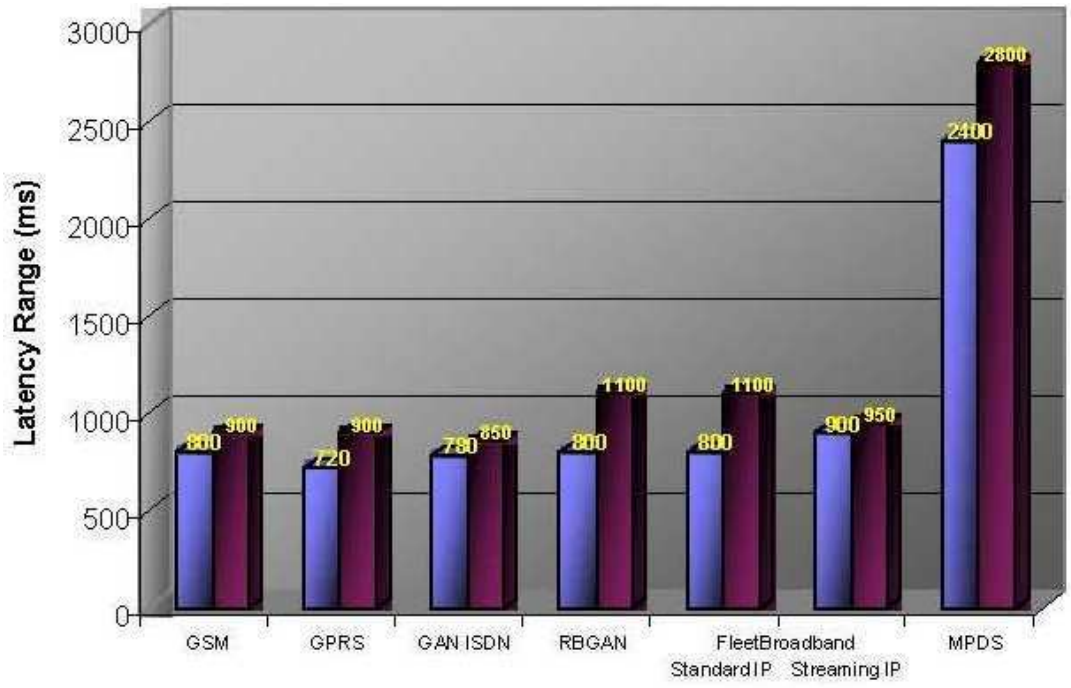


Figure: Latency in Communications Networks

5.9.2 TCP Window Size

A TCP window sets the amount of data that you can send over a particular connection before an acknowledgment is required to confirm receipt.
The primary purpose of a TCP window is to control congestion. An end-to-end connection (for example host-to-server) may have a bottleneck that reduces the throughput of data. If the transmission is too fast, data is lost at the bottleneck. The TCP window reduces the transmission speed to a level where congestion and data loss do not occur. This is particularly important over TCP networks such as Inmarsat as data loss results in retransmission and additional costs.
TCP window size is also important for the Inmarsat network as satellite networks have greater latency than terrestrial networks and waiting for TCP window acknowledgements can reduce the optimal bandwidth significantly. A smaller window size is therefore recommended over Inmarsat.

Recommendation: Inmarsat recommends that you set the TCP window size to 128kbytes on the vessel network.

TCP window size is set within the Windows registry settings in Hex format – 0001ffff being 128kBytes. However, in order to enable TCP window sizes greater than 64kbytes window scaling also needs to be enabled. This is done by modifying the TCP 1323Opts registry setting to 1.
To make both of these changes simply copy and paste the following script into a text editor (such as Windows Notepad), and save it as a **.reg** file (for example windowsize.reg).

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
"TcpWindowSize"=dword:0001ffff
"Tcp1323Opts"=dword:00000001
```

Once the file is saved, double click the file and the changes will be applied. You will need to restart the system for the changes to take effect.

5.9.3 MTU, MSS and RWIN

5.9.3.1 MTU (Maximum Transmission Unit)

The Maximum Transmission Unit (MTU) is the size of the largest packet (or frame) that can be transmitted for a particular network connection. A higher MTU results in higher bandwidth efficiency. The actual MTU for a network connection is negotiated by the network and is determined by the device in the network with the smallest MTU. The largest MTU value for standard Ethernet is 1500 bytes and the default Windows MTU size is the same – 1500 bytes.

Recommendation: Inmarsat recommends that clients should be configured for an MTU of 1360 bytes.

The MTU size can be configured using an application such as DrTCP which is available for download at http://www.dslreports.com/drtcp

5.9.3.2 MSS (Maximum Segment Size)

The Maximum Segment Size (MSS) is the maximum number of data bytes that can be transmitted in a single packet. The MSS size in bytes therefore corresponds to the MTU size minus the IP headers which for TCP and UDP are 40 bytes and 28 bytes respectively.

5.9.3.3 RWIN

The TCP Receive Window (RWIN) size is the amount of received data (in bytes) that can be buffered at any one time on a connection. The sending host can send only that amount of data before waiting for an acknowledgment and/or window update from the receiving host. The RWIN is dynamically changed during a connection by the TCP slow start algorithm. It is important that the initial value for RWIN is not set too low.

OS	Default value	Change required for Inmarsat?
Windows XP	64KB	Yes – change to 128KB
Windows 95	8KB	Yes – change to 128KB
Windows 98	8KB	Yes – change to 128KB
Windows Me	8KB	Yes – change to 128KB
Windows 2000 (pre-SP4)	8KB	Yes – change to 128KB
Mac	64KB	Yes – change to 128KB
Linux 2.6	54KB	Yes – change to 128KB

Table: RWIN Default Values and Settings

The TCP Receive Window size can be configured using an application such as DrTCP which is available for download at http://www.dslreports.com/drtcpU

5.9.4 Quiescent Mode

This section applies to Standard IP only.

When you use applications that send or receive data in bursts, the Inmarsat resourcing algorithm introduces delays. These occur when a connected Inmarsat terminal does not send any data for a period. During these times, the terminal is described as being in quiescent mode.

The following is an explanation of one way in which quiescent mode can be activated:

1. A terminal connected to the Inmarsat network maintains a queue of traffic that is waiting to be sent over the network.
2. If the queue size changes significantly, the terminal sends a status message to the network, asking for an appropriate amount of resource so that the terminal may clear its queue.
3. The network allocates the resource.
4. The terminal sends the data in the queue in the given time slots.

This process of obtaining the resource causes a delay in the traffic and the terminal returns to quiescent mode after a period of approximately two minutes.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.9.5 TCP/IP Slow Start

5.9.5.1 TCP Slow Start Overview

TCP provides its reliability partially through the use of the slow start algorithm. As its name suggests, TCP slow start affects the start of each connection, sending data slowly until it detects that the network can receive a greater volume. However, slow start is re-activated on a connection in the event of packet loss. This behaviour is determined by the TCP window size which determines how many packets can be in progress across the network, without an acknowledgement being received from the other end of the connection.

Slow start can mean that the full bandwidth available on a connection will not be utilised for 10-15 seconds with the result that the perceived performance for a TCP-based transfer is better for large files than for smaller files as shown below in Figure below.

Inmarsat recommends the use of TCP Accelerator (also known as TCP Performance Enhancing Protocol or PEP) to overcome the adverse impact of the TCP Slow Start algorithm when used with small files. Further information on the use of TCP Accelerator is given below in Section 6.6, entitled TCP Accelerator (TCP PEP).

Figure: TCP Slow Start

5.9.5.2 FTP Slow Start

FTP is generally used for transferring large amounts of data. When an FTP file transfer is initiated the first action is to connect to the FTP server. A TCP handshake then takes place after which a number of FTP commands are sent back and forth, followed finally by the data.

The FTP data stream will progressively ramp up, until the full bandwidth of the connection is used. This will continue until the data transfer is completed, or packet loss occurs.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.9.5.3 HTTP (Web Browsing) Slow Start

Web browsing can be affected by a combination of slow start and the Inmarsat resource management.

When downloading a web-page, a web-browser will typically make a number of connections to the server, each connection downloading a part of the page (each image or frame could be downloaded in a separate connection, for instance).

Multiple, small connections have an overhead in that the connection has to be set-up before data can be sent and received, and then the connection dropped. To download a 2KB image, which would require 2 data packets, requires an additional 5 packets in overhead for setting up and dropping the connection.

Each of these connections is affected by the TCP slow start algorithm. In addition, if a web page is downloaded and reading it takes more than a couple of minutes, the terminal will switch into quiescent mode and so the request for the next page will be affected by the resource management algorithm.

Most browsers and servers now support HTTP 1.1, which allows for multiple requests to be sent as part of the same connection. However, some browsers do not make best use of this feature. More can be found on configuring browsers later in this document.

5.9.6 TCP Accelerator (TCP PEP)

5.9.6.1 About TCP Accelerator

TCP Accelerator (also known as TCP PEP) is a free software which has been tested and proven to improve the performance of TCP applications over the Inmarsat network. TCP Accelerator boosts the upload speed of all TCP traffic by up to 300% (depending on file size), with an average increase across all applications of 40% - 80%.
TCP Accelerator is of particular benefit to activities which send short bursts of data over the network, such as Internet browsing and email.
The adjustments made by TCP Accelerator include:

- Modifying TCP window settings by changing the window size to allow a larger amount of data to be carried at any point in time over the network.
- Optimising the MTU size for the Inmarsat network
- Negating TCP slow start behaviour, further deteriorated by the round trip time between the terminal, satellite and ground segment.

5.9.6.2 TCP Accelerator Solutions

There are three types of TCP Accelerator solutions available from Inmarsat for use over the Inmarsat network. These are:-
TCP Accelerator Client. A client application which is installed in the terminal or the attached server. The client application optimises the flow of data in the reverse direction from the Inmarsat terminal to the satellite through to the ground station.
TCP Accelerator Network. A server-based application for non-VPN users. This is installed in the Inmarsat network and together with TCP Accelerator client enhances performance in the receive/download direction.
TCP Accelerator VPN Enterprise. A server-based application for VPN users. This is installed within the Enterprise site, and together with TCP Accelerator Client, enhances performance in the receive/download direction.

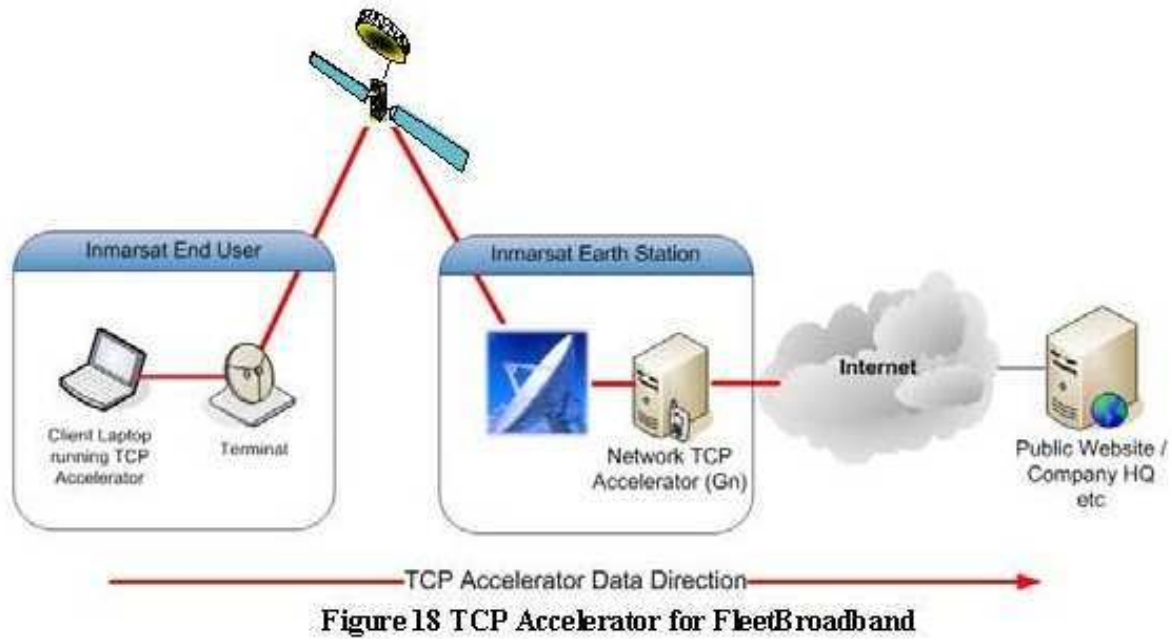


Figure: TCP Accelerator for Inmarsat

The client application can be downloaded and installed on Windows and MAC operating systems from: http://www.inmarsat.com/support, click on BGAN or Fleet Broadband, then click on TCP Accelerator..

5.10| Connecting Peripheral Devices to the Inmarsat Terminal

5.10.1 DHCP - Address allocation

Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses, subnet masks, default gateway and other IP parameters.

When a DHCP-configured client (be it a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as the default gateway, the domain name, the DNS servers, other servers such as time servers, and so forth. Upon receipt of a valid request the server will assign the computer an IP address, a lease (the length of time for which the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting and must be completed before the client can initiate IP-based communication with other hosts.

DHCP provides three modes for allocating IP addresses. The best-known mode is dynamic, in which the client is provided a "lease" on an IP address for a period of time. Depending on the stability of the network, this could range from hours (a wireless network at an airport) to months (for desktops in a wired lab). At any time before the lease expires, the DHCP client can request renewal of the lease on the current IP address. A properly-functioning client will use the renewal mechanism to maintain the same IP address throughout its connection to a single network, otherwise it may risk losing its lease while still connected, thus disrupting network connectivity while it renegotiates with the server for its original or a new IP address.

The two other modes for allocation of IP addresses are automatic, in which the address is permanently assigned to a client, and manual, in which the address is selected by the client (manually by the user or any other means) and the DHCP protocol messages are used to inform the server that the address has been allocated.

The automatic and manual methods are generally used when closer control over IP addressing is required (typical of tight firewall setups), although a firewall can typically be configured to allow access to the full range of IP addresses that can be dynamically allocated by the DHCP server.

The DHCP server in either the Inmarsat terminal or router (depending upon the operating mode chosen - NAT mode or Modem mode) dynamically allocates a private IP address to each user connected to the Ethernet or WLAN interface up to the maximum number of users allowed by the terminal specification. The DHCP server maps the IP address to a network address for full Network Address Translation (NAT) and Port Address Translation (PAT). Each user can therefore open a separate data connection through the Inmarsat terminal.

If Port Forwarding is to be implemented (see Section 7.4 below) then DHCP automatic address assignment must be overridden and a local static IP address manually assigned.

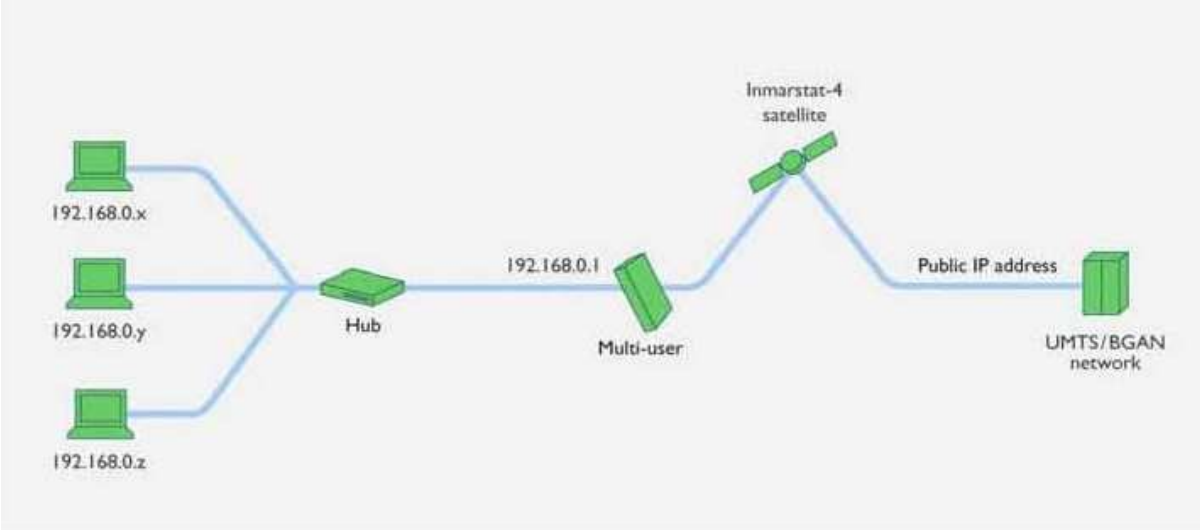
5.10.2 Network Address Translation (NAT) Mode

the connected devices. Alternatively, you can manually configure the IP addresses using your operating system's administrative tools.

When using NAT mode in order for shore-to-ship initiated connections to successfully work port forwarding must be enabled and configured on the Inmarsat terminal - see Section 7.4 below entitled Port Forwarding.

If multiple users are connected to the Ethernet interface, the terminal allocates a private IP address to each device connected to it from its pool of private IP addresses.

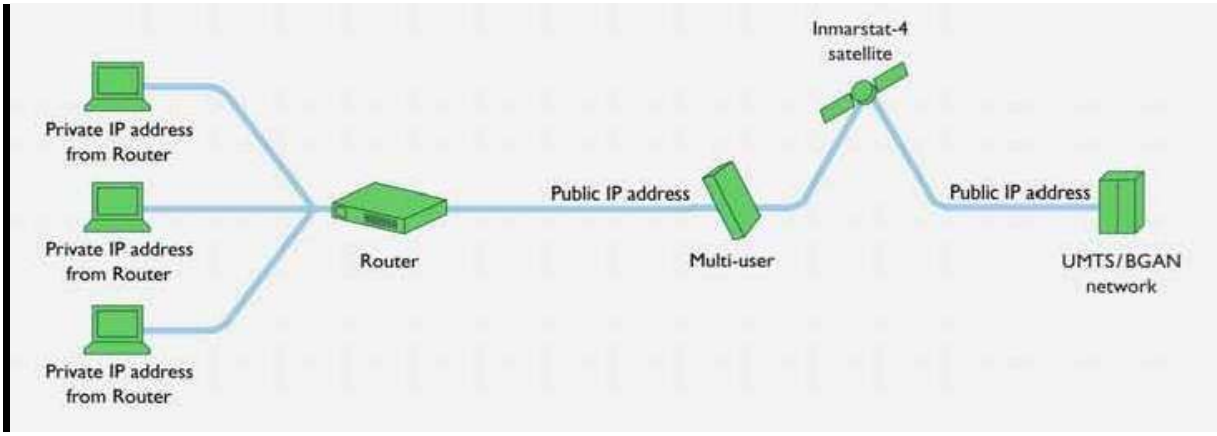
The following diagram illustrates how multiple private IP addresses allocated by the terminal correspond to one public IP address on the network. In this mode each user shares the same Standard or Streaming IP connection.



5.10.3 Modem Mode

In Modem mode, the terminal does not allocate IP addresses to the connected devices. A single public IP address is allocated by your Inmarsat Service Provider to the device connected to the Inmarsat terminal which may be a computer if a single user is connected to the terminal, or a router if multiple users are to be connected to the terminal's LAN interface. If the terminal is connected to a router, the router can then allocate private IP addresses to connected devices from its own pool of IP addresses.

The following diagram illustrates how multiple private IP addresses allocated by the router correspond to one public IP address. If multiple users are connected to the Ethernet interface over a router, only one user can request a Standard IP connection.



5.10.4 Port Forwarding

located on your network behind your router or firewall. Examples of servers requiring port forwarding are web-servers, FTP servers, SMTP servers, computers running telnet, etc.

Every device on a network has an IP address and every IP address has several ports so that a single IP address can be used by multiple applications to send and receive data at the same time. When a network device sends data to another network device, it sends it from a port on one IP address to a port on another IP address. A port can only be used by one application at a time.

When an external network user sends data to the public IP address of a router, the router needs to know what to do with the data. Port forwarding simply tells the router which device on the local area network to send the data to. Once the port forwarding rules are set up the router is able to accept data from a public IP address:port number and route that data to an internal IP address:port number.

Fleet Broadband can be configured for port forwarding and in fact must be configured for port forwarding if more than one device is to be attached to the terminal.

5.10.5 IP Connections Explained

5.10.5.1 About PDP contexts

The Inmarsat Network manages resources using Packet Data Protocol (PDP) contexts.

When you open an IP data connection, a PDP context is opened automatically. This PDP context must be established in the Inmarsat terminal and Inmarsat core network for you to be able to transfer data across the network. A PDP context defines connection aspects such as routing, Quality of Service (QoS), security and billing between the terminal and network.

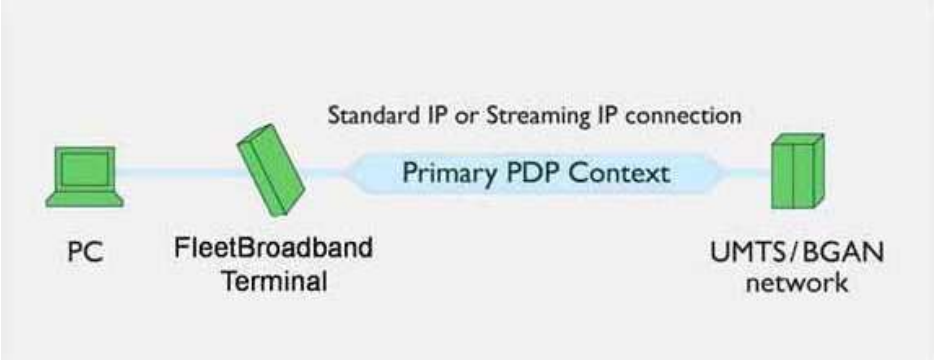
When you first open a PDP context, the terminal requests sufficient radio resources (that is, power and bandwidth) to support the context activation procedure. Once the resources are allocated, the terminal sends the activate PDP context request to the Inmarsat core network. This request includes key information about the Inmarsat terminal, for example:

- the PDP address (which may be, for example, an IP address).
- the PDP type (that is, static or dynamic address).
- the QoS requested for this context – standard or streaming at the selected data rate.
- the Access Point Name (APN) of the external network to which connectivity is requested.
- your SIM card's identity number (IMSI).
- any necessary IP configuration parameters (for example, security settings).

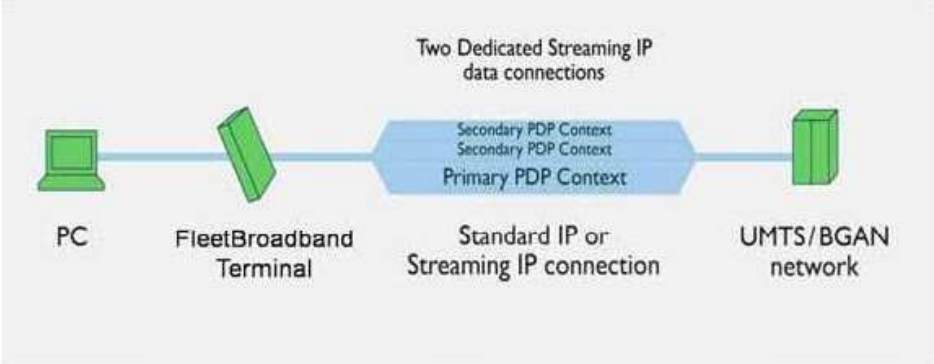
On receiving the Activate PDP Context message, the Inmarsat core network checks your subscription record to establish whether the request is valid. If the request is valid, a virtual connection is established between the terminal and the Inmarsat core network and data transfer can then take place between the terminal and the external data network.

5.10.5.2 Inmarsat and PDP contexts

you open to send or receive traffic over the Inmarsat network. These contexts can either be primary or secondary.
If you open a Standard IP data connection or one of the pre-configured Streaming IP data connections in Inmarsat, the Inmarsat terminal opens a primary PDP context, as shown below. Primary contexts can each connect to a different APN and each get a public IP address.



If you open a dedicated Streaming IP data connection, dedicated to a particular application, the Inmarsat terminal opens a secondary PDP context specifically for this connection as shown below:



A secondary context is always associated with the primary PDP context open on the interface and shares the APN and IP address with the primary context. However, the secondary PDP context can have a different QoS from that of the primary PDP context.
Each terminal has a different method of managing PDP contexts and supports different combinations of primary and secondary PDP contexts.

5.10.5.3 About Inmarsat Network IP addressing

When your Inmarsat terminal connects to the Inmarsat network it is assigned a IP address by your Inmarsat Service Provider. This is the "public-facing" IP address. This IP address can be public or private and static or dynamic. Dynamic configuration is carried out automatically.

You need a public static IP address over Inmarsat in the following situations:

- when running web-servers, mail-servers, or FTP servers behind the Inmarsat terminal in a remote-office or small-office/home-office (SOHO) deployment.
- when operating certain sophisticated SCADA/unattended devices
- when operating certain VPNs that require a static IP addressing scheme.
- when using IP Telephony and video conferencing

5.10.5.4 How static IP addressing is provisioned

Your Local Geoborders Branch or Service Provider normally provisions your SIM card to use public static IP addressing by assigning a username and password to the SIM card ID. Note this is usually provisioned with the default Access Point Name (APN) for your Service Provider.

In most cases your SIM card is provisioned to use public static IP addressing automatically. In very few cases it may be necessary for you to specify static IP addressing manually at the connection stage.

You will need a private static IP address - usually part of setting up a user-requested closed network over Inmarsat - when you wish your vessels to be automatically part of your corporate network by being assigned a specific range of IP addresses that match your internal networks. This usually requires your company to set up a dedicated VPN connection between your company and the DP PoP.

If VPN's form part of your set-up then this type of set-up can help to remove the unnecessary overheads that VPN's create (sometimes up to 50%) that increase the costs of communication as well as reduce overall throughput – see Section 4.5 above for more information.

5.11| Maintenance, Support and Security Procedures

5.11.1 Training and Handover

The integration of Inmarsat into your vessel communications networks can bring a huge range of benefits and efficiencies to your day-to-day vessel operations. However, the extent to which these benefits and efficiencies can be realised will be determined by the skill and knowledge of the crews that will using these systems. It is therefore imperative that the implementation of the Inmarsat Inmarsat-enabled communications networks is accompanied by appropriate training for the users of the systems – both on the vessel and at HQ.

Consideration needs to be given not only to the crew on-board the vessel at the time of installation but also to subsequent crews who, upon hand-over, will require the same level of training.

5.11.2 Remote Support

The ability to provide shore-based support for vessel-based networks and computers is one of the most important drivers for the implementation of Inmarsat on ships. This benefit is further enhanced by the ability to run concurrent voice and data sessions on Inmarsat so that voice communication can be maintained while carrying out remote maintenance using the data connection.

Accordingly, all servers, computers and satellite equipment should be made accessible to technical staff residing shore-side for maintenance and troubleshooting. This can be implemented in the following manner:-

- Subscribe to a public (or private if using VPN) static IP address
- Enable port forwarding and appropriate security rights on the network as well as the computer operating system
- Install appropriate remote administrative software on computers and servers such as UltraVNC, PC Anywhere, Remote Desktop and Remote Assistance (the latter two being built-in features of Windows XP).

5.11.3 Error Logging

The Inmarsat range of terminals log all key activities. This log can be accessed using LaunchPad and should be downloaded and saved and/or printed to assist in any troubleshooting activities. An example of a log display is shown below in Figure 19.

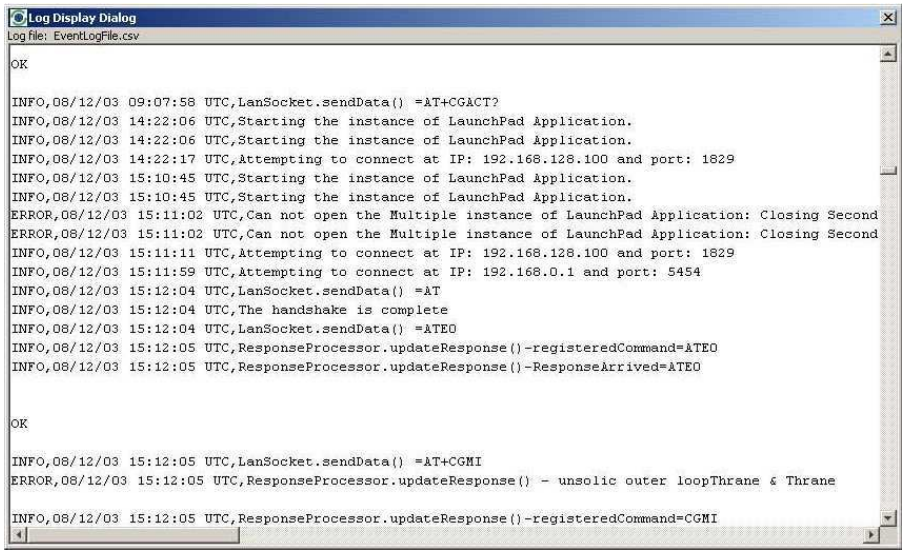


Figure: Inmarsat Log Display

5.11.4 Useful IP tools

Ensure that you are familiar with the various tools and optimisations recommended for use with IP networks, in particular those recommended by Inmarsat for use with satellite communications such as:

- NetMeter/DU Meter
- TCP-PEP
- Dr TCP
- IPConfig

5.11.5 Standby PC and Ghost Images

above discussed the steps you should take to provide effective IT support to remote users. However, from time to time there will be IT failures, often (but not always) hardware related, that just cannot be resolved remotely. In case of such failures it is good practice to have on board one or both of a hot-swappable PC configured for use with the onboard system and a back-up removable disk containing
an exact image of the system set-up (using software such as Symantec Ghost) that can be used to re-install the system.

5.11.6 Operational procedures

Explicit operational procedures must be documented in line with corporate IT network usage policies. The correct operation of equipment, PCs and applications is particularly important in the maritime environment when one considers the frequent changeovers of captains and crew and the varying levels of IT skills and training onboard – see also Section 8.1 above entitled Training and Handover.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.11.7 Access control

5.11.7.1 User levels

Implement appropriate levels of security on PCs and networks differentiating between user and administrative rights.

5.11.7.2 Web access rules.

Control of basic web browsing with multi-user access on-board is the single biggest challenge for network administrators. We suggest that random browsing access (cyber-cafe style) is never allowed without the implementation of the web-browsing optimisations discussed in Section 10.5 below.

5.11.7.3 Pre-emption in case of emergencies

Consideration should be given to the implementation of pre-emptive procedures and over-rides for instances when the Captain or watch-keeping officer requires urgent access to communications in case of an emergency. Such pre-emption could be implemented procedurally or by means of an electrical over-ride installed on the bridge.

5.11.7.4 BIOS and Desktop Locks

Individual computers can be protected from unauthorised access and use by the use of BIOS and desk-top locks.
BIOS passwords can add an extra layer of security for desktop and laptop computers, and are used to either prevent a user from changing the BIOS settings or to prevent the PC from booting without a password. If special settings have been configured on a PC by the corporate IT department they will be protected by a BIOS lock.
A desk-top lock is a computer security and access control application that can be installed and used on a computer to prevent unauthorised persons from accessing files, using programmes and accessing the Internet on that computer.
If you choose to lock your desktop layout, every time you reboot your PC, a desk top lock will restore your desktop icons and bring them back to their original positions as well as return your old wallpaper and screen saver to the background. You can create an unlimited number of desktop layouts for different purposes such as gaming, working, surfing the Internet as well as provide different users with their own desktops.
It is recommended that consideration be given to installing appropriate security and access controls such as BIOS and desk-top locks on all computers that have access to the vessel's communication systems. Inmarsat recommends the use of Easy Desktop Keeper (http://www.softheap.com/desksaver.html).

5.11.8 Scheduling

services and access to the Inmarsat system for personal use, where allowed, by crew members should be scheduled so there is no conflict with vessel operational traffic.

5.11.9 Ship-to-shore Liaison and Escalation procedures

Clear lines of communication and escalation procedures should be put into place so that crew members or shore-based staff know what steps to take and who to call in the event of a problem with the vessel communications system and/or network.
It is suggested that principal points of contact and contact details are identified on the vessel, at HQ and at the Inmarsat Local Geoborders Branch or Service Provider.
Primary and secondary contacts should be identified in case of non-availability of the primary contact and consideration should be given to the implementation of a company escalation procedure to be invoked for outages or problems which are not resolved in a given time-frame.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.12| Communication Cost Management

5.12.1 Develop a traffic profile

It is not sufficient to know just what applications you intend to use - it is equally important to know the nature of traffic you expect to generate. Is the traffic at a constant level like, for example, FTP as shown below in Figure 1 or is it intermittent like, for example, web-browsing as shown below in Figure 2?

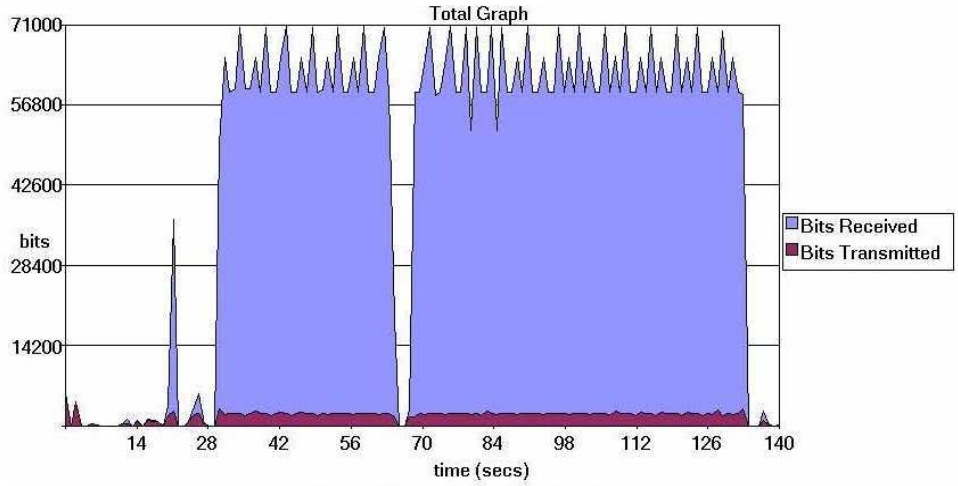


Figure 1: FTP Traffic Flow Profile

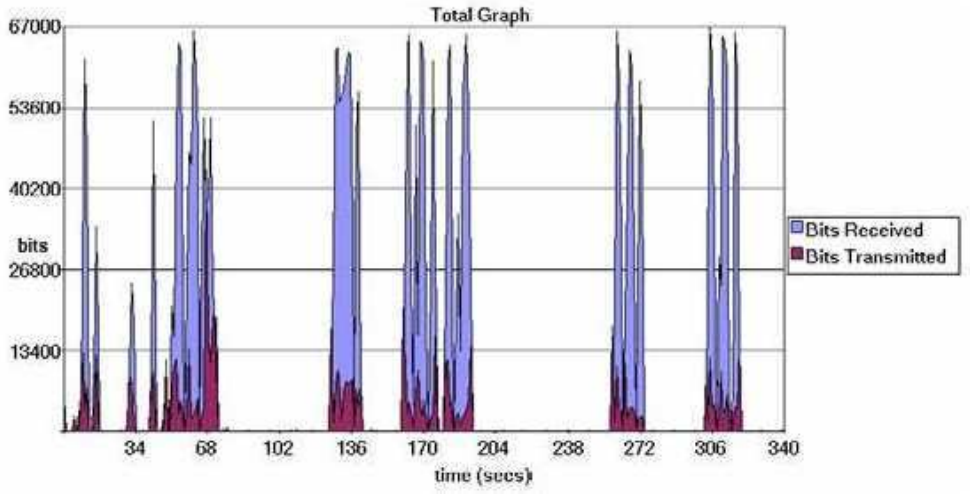


Figure 2: Web-browsing Traffic Flow Profile

The traffic flow profile example given in Figure 20 above shows an efficient use of the channel and suggests that a Streaming IP channel, where costs are determined by time, would be the most cost-effective data connection for this type of traffic.
On the other hand, the traffic flow profile example given in Figure 21 above shows an inefficient use of the channel with many periods when no data is being sent or received. Such a profile suggests that a Standard IP channel, where a costs are determined by volume and not time online, would be the most cost-effective data connection.
It is only by analysing your traffic flow that you will be able to make an informed decision as to the most suitable and cost-effective data connection for each of the applications you wish to use on your network.

5.12.2 Least-cost Routing - Manual and Automatic

Having created a traffic profile for each of your applications you are now in a position to decide which communications routing is the most cost-effective for that application. Such a decision will take into account not only the traffic profile but also the quality of service required, the urgency of the traffic, the charging basis (whether charged by time or volume) and the actual tariff charged.

A least-cost routing analysis can be carried out and implemented manually or, preferably, automatically with the use of least-cost routing applications such as those from:

- Becker Marine UMC
- Dualog
- Livewire – Selector Switch
- Virtek
- SeaWave - Integrator 3.0

5.12.3 Traffic Monitoring Tools

Automated traffic monitoring tools will be a key component of your communications cost management strategy. Such tools may be provided by your Inmarsat DP or are available as third-party solutions and will typically provide functions like:

- access to traffic usage information in as near to real time as possible
- setting traffic "warning" thresholds
- traffic profiling

5.12.3.1 DP Solutions

Check with your DP for the availability of proprietary on-line traffic monitoring tools such as Stratos Dashboard or Vizada Online.

DP-provided tools often incorporate additional management tools such as:

- control over SIM cards and call-time credit for each mobile terminal
- uploading additional credit
- creating groups of end-users
- assigning credit allowances in dollars, either to SIM cards or groups of SIM cards
- receive automatic warnings by email
- ability to activate, deactivate, suspend, un-suspend and make any changes to SIM cards

For the full range of DP value added services please contact your Local Geoborders Branch

5.12.3.2 Third-party Solutions

Several third-party solutions also exist for monitoring the volume and throughput of data transmitted to and from a PC. Some examples that have been tested by Inmarsat are:

- DU Meter http://www.dumeter.com/
- NetMeter http://www.hootech.com/NetMeter/
- IP Consultant http://flyawaycase.com/news/Packet-data.htm

Please visit the relevant web-sites for further information on the functionality available.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.12.4 Automatic Updates

Although it is important to keep your computer up to date with Microsoft updates and virus definitions, they are not always crucial or critical when you are out in the field. However, some of these updates run in the background without you knowing and reduce the bandwidth available for more important applications. In addition, as Inmarsat network use is charged by volume (over standard IP), there are cost implications in how these updates are managed.

All vessel IT equipment will typically have been integrated, configured, updated with the latest software revisions and tested ashore prior to installation onboard. Following installation onboard, the vessel network should be configured so that only one computer downloads the updates which are then locally distributed to all other computers on the network. Such a strategy will be most effectively implemented if all computers onboard use the same applications, anti-virus and anti-spyware solutions.

Tip:

- **MS automatic updates should be disabled not only to control traffic costs but also to prevent operating system configuration changes which affect the overall operation of the PC.**
- **Anti-virus and anti-spyware updates should be kept up to date. However, the frequency of updates should be reduced to weekly rather than daily updates**

To turn off Windows automatic updates:

- Right-click on My computer, and select Properties from the sub-menu.
- Click on the Automatic updates tab.
- Select Turn off Automatic Updates.
- Click on Apply, then click on OK.

You can re-enable the updates from the same interface.

5.12.5 Domain Name Server (DNS) Traffic

A Domain Name Server (DNS) is used by most TCP/IP applications to translate Internet names (for example www.inmarsat.com) into Internet Protocol (IP) addresses.

So, to use Inmarsat as an example, instead of having to type in http//161.30.215.56 every time we want to look at the Inmarsat web-site we can simply type www.inmarsat.com into our web-browser and the Domain Name Server translates the domain name into the IP address of the server which hosts the web-site. The web-browser then uses the IP address to connect directly to the server.

If we didn't use a DNS or for any reason the DNS was not working then we would always have to type the full IP addresses of the web-site that we wished to browse instead of using the much more user-friendly domain name.

However, each DNS lookup can generate between 1 and 2 kbytes of traffic. The most effective way to reduce this traffic is to run a DNS caching server on the remote (vessel) side of the satellite link. This may only be practical if using a LAN configuration. The caching server accepts local look-up requests from other devices on the network and only looks up across the satellite link if it is unable to satisfy the look-up from its own cache. Cached DNS lookups are normally valid for 2 or 3 days; this is configurable per domain, by the owner of the domain.

An alternative to DNS caching is to avoid using DNS for frequently-used device names. You can do this by putting an entry in the HOSTS file on the client machine. The HOSTS file, which also contains instructions on populating the file, can be found at C:\WINDOWS\system32\drivers\etc.

DNS caching and changes to the HOSTS file should be carefully managed as configuration errors will result in users being unable to access web-sites using domain names and having to use IP addresses.

Tips:

- **Use a DNS caching server on the vessel if possible**
- **Use entries in the HOSTS file for further traffic reduction.**

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.12.6 Using Web-caching

server will only retrieve a web page if it does not have the page in its cache. For sites with the same graphics (for example, a company logo) on many pages, the graphic will only be retrieved once, rather than for every page.

Web-caching servers are normally installed on LANs. However, all browsers incorporate a web-cache, which serves the same purpose for single-user set-ups.

Note that cached data sometimes expires which means that it from time to time it may need to be reloaded.

Tips:

1. **Use a web-caching server if possible**
2. **Ensure your browser's web-cache is active and as large as possible**
3. **If possible before using the Inmarsat network connect to all sites that you are likely to use over Inmarsat. This will preload your cache with the images etc from these sites.**

5.12.7 Reducing Unnecessary LAN Traffic

5.12.7.1 Block unwanted traffic

When a client computer is connected to a Inmarsat terminal with a network cable, the computer considers itself part of a LAN. The Inmarsat terminal is treated as if it were a router on that LAN. Computers may also be connected to a local LAN, with its own router, that is in turn connected to the terminal.

Devices on a LAN generate traffic which can inadvertently and unnecessarily be sent through the router/terminal. This traffic consists mainly of broadcast messages and multicast frames which are searching for resources such as printers or shared drives. Microsoft Windows networks typically generate traffic of this type.

Unwanted traffic can be defined as any traffic other than that which is important. Typical examples of traffic that fits this category are:

- Network broadcasts from applications looking for network devices, such as printers.
- Status updates from applications
- Windows Server Message Block (SMB) traffic. By default, Windows generates a lot of SMB traffic which can result in poor file server performance. However, some of this traffic is superfluous and can be reduced.

5.12.7.2 Polling/update checks

In most cases, Inmarsat recommends that you configure the router to disable this traffic. Sometimes the traffic is required because the remote LAN is part of a larger LAN using the satellite link as a bridge. In this case, some routers can be configured to allow this sort of traffic, but not allow the traffic to initiate the link (that is, the traffic is allowed only when the link has been established). Alternatively, spoofing techniques can be implemented at each end of the link. These techniques cut down on unnecessary network traffic by the use of intelligent caching.

Stand-alone machines connected directly to a Inmarsat terminal do not usually suffer from these problems. However, Windows systems using the default

configuration can experience problems because Windows installs most common protocols (as well as TCP/IP) by default and as a result unexpected traffic may be generated.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.13| Applications Optimisation

5.13.1 Voice/VoIP

All of the Inmarsat terminals support circuit-switched voice at 4kbps. Analysis shows that Skype, the most popular voice over IP technology, requires 60-65kbps and Net-to-Phone requires 20-24kbps. In addition in certain circumstances the use of Skype can render a network vulnerable to certain security breaches - for more information see www.securecomputing.com/index.cfm?skey=1602.
Inmarsat therefore recommends that for voice calls the Inmarsat direct dial voice service is used in preference to IP-based telephony solutions.

5.13.2 Fax

Group 3 and Group 4 fax calls can be transmitted and received on terminals supporting 3.1kHz audio (FB250 and FB500) and ISDN (FB500 only) respectively. However, Inmarsat has found that fax over IP applications provide a more cost-effective solution to the transmission and reception of faxes using Inmarsat than using circuit-switched solutions such as Group 3 and Group 4 fax technology. Fax over IP solutions are provided by several companies including:

- RTE FaxBox http://www.rte-software.com/gb/rtefax_smtp.asp
- E-fax http://home.efax.com/s/r/uk_home?CMP=OTC-uk
- On-Go http://www.on-go.com/insol.html

5.13.3 Chat

There are many chat and text-based messaging applications available on the Internet. If a messaging service is to be used in conjunction with the Inmarsat service then the choice of messaging platform should take into consideration any control features within the application and the overheads associated not only with the chat but those associated with potentially keeping the chat sessions alive for periods of several days.

5.13.4 Email

5.13.4.1 Improving email performance

In general, the SMTP, POP and IMAP protocols do not offer compression, although IMAP4 allows retrieval of headers only.
The most effective method of optimising email clients over these protocols is to reduce the amount of data that is sent and received. This also applies to proprietary protocols. The following hints and tips are generic and apply to all protocols and clients. The rest of this section concentrates on optimising some of the most commonly used clients:

- Use IMAP servers rather than POP3 servers and enable the viewing of message headers rather than downloading all messages.
- Disable regular automated checks for new mail to reduce traffic.
- Disable the download of messages whilst they are being previewed to reduce traffic.
- Ensure that messages are sent as text, rather than as HTML, to reduce message size. An HTML message can be up to twice the size of a text message.
- Disable signatures to reduce message size.
- Disable read receipts to reduce traffic.
- Compress attachments to reduce message size. (Also, consider converting attachments to text files, to reduce message size.)
- Enable connection selection on start up.
- Enable offline use, so that message delivery is a controlled activity rather than taking place as a background activity.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.13.4.2 Optimising email clients

Some Local Geoborders Branches provide dedicated email facilities, which are configured to work more effectively over a satellite link and therefore improve on those provided by a conventional terrestrial ISP. In addition, as the DP hosts the mail service, traffic can bypass the Internet thus providing extra resilience and performance improvements.

General principles

Inmarsat recommends that you use a Standard IP data connection for email. The Standard IP data connection opens by default when you register with the network and is sufficient for most email requirements.

Compression

The most cost-effective way to send large attachments over a packet network that is billed by volume or time is to compress the file with a standard utility such as:

- WINZIPTM, available from http://www.winzip.com/ or
- WinRAR, available from http://www.rarlab.com/

You can then FTP the file to a designated FTP server and alert the recipient by email to retrieve the file locally. Many email clients when sending attachments via SMTP will substantially increase an attachment's size, sometimes by as much as 50%. Compressing attachments is only of benefit if the content is not already compressed, and the if the recipient has a utility to uncompress the attachments.

Contact your DP for further advice in this regard.

5.13.4.3 Optimising Outlook Express

Outlook Express supports both POP3 and IMAP4 protocols. Neither of these protocols provides any compression of data over a communications link. You can optimise the performance of these protocols, as follows:

- Switch off **Check for mail every x minutes** option, or set the value to several hours. Checking for mail when there isn't any generates up to 6KBytes of traffic. By checking for email only when necessary, you can reduce costs.
- Switch off **Send and Receive messages at start-up**. This allows queuing or sending of batches of mail.
- Disable **Automatic download of messages when in the viewing pane**. This stops messages being downloaded as you browse the headers.
- Send plain text messages only. If you use bold, underline and non-standard fonts more data is used than plain text.
- De-select the **Send messages immediately** option. You can queue messages enabling them to be sent all at once rather than initiating a new connection for each message.
- **Do not include the original message in your reply**. This reduces the amount of data sent.
- **Do not include read receipts.** Read receipts are designed to allow the sender of the message to be notified when the recipient has opened the message. As this generates extra traffic, Inmarsat recommends that you switch them off.

Tip:

1. **IMAP4 transmits email twice. The email is first sent to the SMTP server and then to the IMAP server to be placed in the Sent Items folder. You can turn this feature off by un-checking the Save copy of sent messages in the 'Sent Items' folder check box.**
2. **Outlook over IMAP4 allows the client to synchronise selected folders to the local machine. This feature is controlled on the window shown when the IMAP account is selected from the left hand panel. Turn synchronisation off for all folders to avoid unnecessary downloads.**

5.13.4.4 Optimising Eudora 5.1

Eudora 5.1 supports both POP3 and IMAP4 protocols. Neither of these protocols provides any compression of data over the communications link. You can optimise the performance of these protocols, as follows:

- Download part of a message (over POP3). This has the benefit of appearing to download only the header (if set correctly), and of giving you the option of deleting a message that may contain a virus without downloading it. You are prompted to skip messages over a certain size; Inmarsat recommends that you skip messages over 3KBytes.
- Note: Although this setting suggests that you are skipping messages over a specified size, in fact the programme skips the remainder of the message after the first 3KBytes has been downloaded.
- Leave email on the server. This has the advantage of enabling you to retrieve the message later, or downloading a duplicate copy if you lose the original. The disadvantage is that you could download a duplicate copy of an existing message. Inmarsat recommends that you download what is required, and delete what is not from the server.
- Send plain text messages only. If you use bold, underline and non-standard fonts more data is used than plain text.
- Do not include signatures. Signatures impose an extra overhead.
- Send messages together. This allows email to queue, which reduces the number of SMTP connections needed to send messages.
- Check for mail manually (or set the automatic check function to check every few hours). Checking for email only when necessary can reduce costs.
- Do not enable read receipts. Read receipts are designed to allow the sender of the message to be notified when the recipient has opened the message. This generates extra traffic. Read receipts are disabled in Eudora by default.

5.13.4.5 Optimising Mozilla Thunderbird

same modifications can be carried out to ensure that this client works optimally over Inmarsat.

- Switch off Check for mail every x minutes, or set the value to several hours. Checking for mail when there isn't any generates around 6KBytes of traffic. By checking for email only when necessary, you can reduce costs.
- Switch off Send and Receive messages at start-up. This allows queuing or sending of batches of mail.
- Send plain text messages only. If you use bold, underline and non-standard fonts more data is used than plain text.
- Unless you want your messages available offline, disable offline downloads. Uncheck the Make the messages… and When I create new… check boxes.
- Disable some of the advanced options for extra bandwidth savings. Uncheck Block loading of remote images, and disable the return receipts option.

Tip: IMAP4 transmits email twice. The email is first sent to the SMTP server and then to the IMAP server to be placed in the Sent Items folder. You can turn this feature off by un-checking the Save copy of sent messages in the 'Sent Items' folder check box.

5.13.4.6 Using specialised email solutions

There are several companies that provide email services or middleware specifically for wireless networks. Middleware is a term used for software that provides a link or bridge between two applications or environments. Rather than develop complete messaging hub solutions for satellite systems, some specialist companies have developed components that integrate with the popular corporate systems. These solutions allow closer integration with existing corporate messaging systems, whilst still providing features that benefit the remote user.

On a per email basis, it is actually far more cost-effective to check your email through the many optimised solutions on offer from Local Geoborders Branches or middleware providers such as.

- Stratos Amos Connect www.stratosglobal.com
- SkyFile (Vizada) www.vizada.com
- Fly Carrier/Victoria (MVS) www.mvsusa.com
- Becker Marine UMC www.umcglobal.net
- Virtek www.virtek.no
- Satmail www.kddi.com

It is also possible to purchase hubs that can be sited at corporate headquarters in order to provide access for remote users directly into corporate systems, rather than routing through a third party.

These solutions variously offer some or all of the following benefits:

Extra resilience

If a data link is broken during the transmission of messages, standard software will re-start the transmission from the beginning. Specialised software is able to continue this transmission from the point it stopped.

Message filtering

Specialised software enables you screen email before it is downloaded. You can use this simply to prevent large messages from being downloaded, or you may be able to check who is sending messages and only allow messages through from known sources.

Least-cost access

It may be possible to save on costs by choosing a different class of connection, based on the volume and frequency of email transactions. For example, a connection charged by time may be cheaper than a connection charged by volume for larger volume email transactions. In addition, specialised software can provide the ability to automatically select the cheapest network.

Batching and compression

Specialised services can provide automated batching and compression matched to the tariff structure, ensuring that messages are transmitted in the most cost effective way.

5.13.4.7 Web-mail

Web-based email solutions (such as Hotmail, MSN etc) are simple to implement and have become extremely popular with users. However, they are not really suited to the mobile communications environment as most web-based email solutions require direct Internet access and generate significant amounts of data traffic for every page that is accessed or refreshed – simply accessing a home/log-on page generates substantial data even before emails are sent or received.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.13.5 Web browsing

5.13.5.1 Middleware

Third-party middleware solutions provide a cost-effective means of controlling and optimising access to web-based service in the Internet. Such control and optimisation is achieved by the use of several techniques including:-

Caching

Caching is a useful tool for the reduction of external traffic. A web-caching server will only retrieve a web page if it does not have the page in its cache. For sites with the same graphics (for example, a company logo) on many pages, the graphic will only be retrieved once, rather than for every page.

Image compression

Images contained in web-pages can be substantially compressed for initial viewing and the full image downloaded only if required

Operation of white-lists and black-lists

List of sites that cannot be accessed (black-list) or list of the only sites that can be accessed (white-list)

Content filtering

Up to 90% of unnecessary web-page content (such as pop-ups, adware etc.) can be filtered out prior to download and consideration should be given to the blocking of all streaming media.

Traffic Monitoring

Maximum traffic volumes or costs can be pre-determined and appropriate alarms set
when these levels are reached.

Many of these functions can be carried out using Local Geoborders Branch value added solutions or third-party solutions such as those from:-

- Virtek www.virtek.no
- Becker Marine UMC www.umcglobal.net

Please contact your service provider for details of DP-provided solutions.

5.13.5.2 Structured Browsing

The ubiquitous browsing that everyone does today can be described as casual, random, interactive and unstructured. It is basically inefficient in terms of the time required and the volume of data downloaded proportionate to the information desired but is suitable for a wide range of requirements in the framework of widely available low cost Internet access.

However, in the absence of low cost Internet access it is necessary to "optimise" the browsing experience by reducing the time required and reducing the volume of data downloaded it is. One powerful optimisation is the use of structured browsing which restricts web access to pre-designated sites (white-lists) that are additionally pre-downloaded usually at the local intranet of the company and further refined by stripping it of any advertisements, risky links and dangerous attachments.

So, structured browsing has the power to deliver a near-real-time browsing experience - but cost effectively. Structured browsing solutions are available from several companies including:

- IORA www.iora.com
- Infonica www.infopark.de

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.13.5.3 Web Browser Optimisations

Web-browsing performance is influenced by a number of factors:

- The number of connections opened to the web-server.
- The size of data on the web-site.
- The complexity of the web-site.
- Whether the client and server use pipelining.
- How the page is rendered by the browser (can give an appearance of speed).

During testing over Inmarsat it was found that different browsers gave very different results when browsing the same web-site. Using the Inmarsat home page www.inmarsat.com as an example it was found that:

- **Mozilla Firefox 1.5 was 20% faster than Internet Explorer 6.0.**
- **Opera 8.5 was 35% faster than Mozilla Firefox and 50% faster than Internet Explorer 6.0.**

It is believed that the difference in performance was due to the use of pipelining and internal delays between pipeline requests which differed in the three browsers.

Pipelining is a technique in which multiple HTTP requests are transmitted to a single network socket (TCP connection) without waiting for the corresponding responses. Pipelining is only supported in HTTP 1.1, not in 1.0. The pipelining of requests results in a dramatic improvement in page loading times especially over high latency
connections such as satellite Internet connections.

this seems to be borne out by the simple tests that were performed by Inmarsat. Opera uses pipelining with four simultaneous TCP connections by default. It should be noted that some web-servers are configured to prevent browsers using more than two TCP connections and so it may not always be possible to take advantage of Opera's four TCP connections.

Firefox does not use pipelining by default but can be configured to do so using the instructions outlined below. Inmarsat tests found that pipelining improved the performance of Firefox but did not make it as fast as Opera. Internet Explorer does not use pipelining.

Enabling Mozilla Firefox Pipelining

To enable Mozilla Firefox pipelining:

• Start up Firefox.
• Type **about:config** into the address bar, and press enter. You will see a page of configuration settings.
• Change the following:
  - Set “network.http.pipelining” to true
  - Set “network.http.proxy.pipelining” to true
  - Set “network.http.pipelining.maxrequests” to 8

Optimising Internet Explorer for MAC

To optimize Internet Explorer for MAC, select Preferences > Advanced, and change the following:

- Check the Support Multiple Connections check box.
- Check the Show Server Messages check box.
- Set Max Connections to 4.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.14| Operating System Optimisation

5.14.1 Windows OS Optimisations

The following applications are generally configured to connect to the Internet:

- Windows Updates
- Messengers – MSN messenger, Yahoo, Skype, Googletalk etc.
- Media Players
- Virus checker and others e.g. spyware guards, firewalls etc.

To minimise the network usage of these, carry out the following steps:

Disable Messengers

For example using MSN messenger you should:

- Open MSN Messenger, and select **Options** from the **Tools** menu.
- On the General tab, uncheck **Automatically run…** and uncheck **Allow automatic sign on…**

There will be something similar with all the other messenger clients, look for preferences, options or settings.

Disable Media Player update checking.

For example using Windows Media player you should:

- Open Windows Media Player, and select **Tools > Options > Player** from the main menu.
- Disable Download codecs automatically, and select the option to check for updates once a month.

NOTE: Windows Media Player only checks for updates if it is running, and it does not run by default.

Optimize your virus checker.

Most computers come pre-configured with a virus checker, which updates on a regular basis. It is important to keep your virus checker updated, but sometimes a good idea to control exactly when this happens. Inmarsat recommends the following:

Start your virus checker configuration application and find the preferences section that allows you to control when regular updates happen. Modify as required.

Should a number of users be connected to a single Inmarsat terminal, configure one PC to collect virus updates. Configure other PCs to use that PC for their updates, rather than connecting to the remote update server themselves

Other optimisations

Go through your start-up menu and prevent any applications that are not required from starting automatically. Items on this menu will start when you start your operating system. Removing the application from this menu does not delete the application; you can start it manually when required.

Go through the icons in your system tray, and configure applications that are not required to not start on start-up, and not automatically check for updates.

Use a tool such as ccleaner (www.ccleaner.com) to examine the programs that start when Windows start, and remove as required (advanced users only).

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.14.2 Linux OS Optimisations

There are many Linux distributions in use today, all of which may be installed in a number of ways to provide functionality of a desktop, a server, or a combination of the two.

The default TCP parameters for Linux operate successfully on the Inmarsat network. You can make modifications to these settings by changing values in the pseudo files found in the following directories:

/proc/sys/net/core
/proc/sys/net/ipv4

You can make these changes at any time, but you must make them each time you power on the computer. You can create a suitable script and run it in /etc/rc.local (or the equivalent on your distribution). Some parameters may also be set in the file /etc/sysctl.conf

Application Optimisations

Ensure that only the required applications are enabled by default. On most Linux distributions, you can use the following command to see which applications are starting automatically:

 # chkconfig –list

Pay particular attention to any auto-update routines, as these may download significant amounts of data. These include applications such as RNH (RedHat Network) and up2date.

The following applications are generally configured to connect to the Internet:

- Messengers – MSN messenger, Yahoo, Skype, Googletalk etc.
- Media Players
- Virus checker and others e.g. spyware guards, firewalls etc.

To minimise the network usage of these, carry out the following steps:

Disable Messengers

For example using MSN messenger you should:

- Open MSN Messenger, and select Options from the Tools menu.
- On the General tab, uncheck Automatically run… and uncheck Allow automatic sign on…

There will be something similar with all the other messenger clients, look for preferences, options or settings.

Optimise your virus checker

Most computers come pre-configured with a virus checker, which updates on a regular basis. It is important to keep your virus checker updated, but sometimes a good idea to control exactly when this happens. Inmarsat recommends the following:

- Start your virus checker configuration application and find the preferences section that allows you to control when regular updates happen. Modify as required.
- Should a number of users be connected to a single Inmarsat terminal, configure one PC to collect virus updates. Configure other PCs to use that PC for their updates, rather than connecting to the remote update server themselves

Other optimisations

Go through your start-up menu and prevent any applications that are not required from starting automatically. Items on this menu will start when you start your operating system. Removing the application from this menu does not delete the application; you can start it manually when required.

Go through the icons in your system tray, and configure applications that are not required to not start on start-up, and not automatically check for updates.

Linux tends to clear out its temporary folders on restart and doesn't have a registry in the same way as windows so there is little need for cleaner programs like ccleaner (www.ccleaner.com).

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

5.14.3 Mac OS Optimisations

Mac OSX is UNIX based, so knowledge of UNIX or Linux systems can help when optimising MAC for use over Inmarsat.
The default TCP parameters for Mac OSX operate successfully over the Inmarsat network. You can make modifications to these settings by adding values to the file /etc/sysctl.conf and the performing a reboot.

kern.ipc.maxsockbuf=<num bytes> (The maximum TCP buffer size)
net.inet.tcp.sendspace=<num bytes> (The send buffer)
net.inet.tcp.recvspace=<num bytes> (The receive buffer)

Application Optimisation

Ensure that only the required applications are enabled by default.
Use the Systems Preferences application to find out which applications are run at start-up, on the **Login Items** page. Stop any unnecessary applications from starting.
Other Unix layer applications may start at boot up. You can check these by looking in the folders:

/System/Library/StartupItems (reserved for those provided by Apple)
/Library/StartupItems

To minimise network usage, turn off Mac automatic updates as described below:

- To prevent iTunes from updating, within iTunes choose **Preferences**, and disable **Check for iTunes updates automatically**
- To prevent iPhoto from updating, within iPhoto choose **Preferences**, and disable **Check for iPhoto updates automatically**
- To prevent QuickTime from updating, run the System **Preferences** application, select **Internet and Network > QuickTime**, then **disable updates.**
- To prevent Safari from updating, choose **Preferences > RSS"**. Set **Check for updates to Never**.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

6| Frequently asked questions about BGAN.

What is the Latency for the BGAN Network?
The BGAN network typically provides a Latency of between 900 - 1100 milliseconds.

What can affect the Network and impact email performance?
Helpful tip: You can achieve a more cost-effective and efficient email service by ensuring that your email client/server settings have been optimised for satellite networks. For further assistance, please contact your Local Geoborders Branch (DP). Cause and effect Latency, or delay experienced over the network, impacts the performance of acknowledgements and therefore of packet sizes. The BGAN network typically provides a latency of between 900 - 1100 milliseconds. Jitter This is the range by which the latency of a network varies. The greater the variation the higher the jitter and therefore the higher the impact on the email protocols used. A Standard IP data connection tends to have a higher Jitter than a Streaming IP data connection. Overheads When a protocol sends email, there is an associated overhead, for example in the use of headers and packet acknowledgements. The percentage size of the overheads varies depending on the protocol . Dynamic Packet size Dynamic packet size determines the volume of data that can be sent per packet in comparison to the error correction information. Dynamic packet size varies depending on the protocol, but plays a significant role in FTP. It enables throughput to therefore vary depending upon the quality of the service.

Are short dialling codes supported by BGAN?
Local Geoborders Branches (DPs) are required to provide Inmarsat with the short dialling codes they plan to use along with their full National number.

What is the short code to collect voicemail messages?
Dial 57# to collect voicemail.

Can an SMS be sent to more than one recipient at a time?
Yes. The BGAN LaunchPad system can send an SMS to an unlimited number of selected recipients.

Is each SMS sent charged separately?
Yes. There is a charge for each individual message.

How do I know if BGAN can be used in a particular country?
Inmarsat has a dedicated regulatory team that confirms the licensing situation in all countries. A licensing spreadsheet is available on the Inmarsat Connect website.

Is there a map which shows the edge of BGAN coverage?
The coverage maps are not definite because the edge of coverage is not static. Geo satellites reside within a "box" in space, inside which they drift from one edge to the other (typically 0.5 degree drift). As they drift, so the edge of coverage moves. However, the I-4 Eye will provide an indication of BGAN coverage.

Is a PDA version of BGAN LaunchPad available?
Currently it is possible to use a PDA with the terminal by connecting over the Bluetooth interface. An initial configuration using BGAN LaunchPad is necessary . This involves setting the terminal to automatically open up a standard data session when turned on. A PDA version of BGAN LaunchPad is currently being developed.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Is 'BGAN LaunchPad' able to send a SMS directly after registration?
Once registered, the BGAN LaunchPad software will be active and able to send and receive SMS.

What is the process to set up voicemail?
Dial 57# or +870 772 001 899 from the BGAN network. Then follow the instructions on the recorded voicemail message. The user will be asked to select a PIN number (typically four characters or more) and to state their name. They will then be directed to create a personal greeting for their voicemail. When a new message is received, the network will automatically send a text (SMS) to their terminal. The user can then dial short code 57# to listen to the message.

When I receive an SMS, do I pay for this?
No, the sender pays for the SMS

Can a SMS be sent to a pager service?
Some paging systems have been modified to receive text messages from the local mobile networks. The user will be unable to access the service if they are outside their own country because the numbering scheme (or plan) for pagers is not part of E.164 numbering.

What is the total power output of the I4 satellite?
The total EIRP (Effective Isotropically Radiated Power) that can be allocated to the narrow spot beams is 67 dbW.

Is there global barring available on BGAN?
SIM cards can be barred or disconnected for any location by the Local Geoborders Branch (DP).

How does Voice Over Internet Protocol work, is it point-to-point?
We have an IP bearer that is transparent to applications, VoIP is just one of those. We have tested common VoIP providers such as Skype.

What is the maximum number of bearers in any one spot?
This is dependent on demand for the BGAN service. Inmarsat has the flexibility to dynamically assign spectrum and power where it is needed. Capacity can be adjusted and allocated depending upon demonstrated demand for the BGAN family of services.

What is the purpose of the new 176k streaming rate?
The new streaming rate is aimed at providing flexibility to the current streaming rate options. It is available to users who are price conscious and require high rates of streaming above 128kbps. The 176kbps streaming rate is particularly appropriate for users looking to stream 'talking head' shots or shots with low levels of background movement. The new stream rate will also offer a higher rate of streaming than what is currently available in the rare occasions when congestion occurs by supporting multiple 176kbps streaming connections in one BGAN channel.

Who is the 176k Streaming aimed at?
176kbps streaming will be available to all Hughes 9201 and Thrane E700 terminal users. The Inmarsat streaming services provide a guaranteed pipe for IP based applications, in particular customers with UDP applications such as video/audio streaming use the service eg. Broadcast media and government users.

What are the benefits of the new 176k streaming rate?
The benefits of the new 176k streaming rate relates to the fact a lower streaming rate allows for flexibility for various applications which may not always require the higher 256k or X-stream rates.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Is the 176k Streaming Service a guaranteed streaming rate?
This is a guaranteed 176kbps in the forward and return directions in-line with streaming rates currently available.

Can the new 176k streaming rate be used on existing BGAN terminals?
The 176k streaming rate is accessible with Class 1 terminals only; Thrane & Thrane EXPLORER¿ 700 or Hughes 9201. There is no need to purchase any additional equipment to access the BGAN 176k streaming rate.

Is the new streaming rate automatically added to sim cards?
You will need to contact your Local Geoborders Branch to confirm you are provisioned for the new 176k service to ensure you are billed accurately. As this does not constitute a change of package, there should be no change to your existing contract.

When can the new streaming rate be applied and when does it become available?
176k Streaming is due to be launch on June 2nd 2010.

Is there a requirement to upgrade the software for existing BGAN terminals?
There is no need to upgrade your terminal firmware to use the new service.

Do we need to upgrade the LaunchPad to take into account the new streaming rate?
A new LaunchPad version including 176 Streaming support will be available from the 2nd June for Windows and MAC OSX on the Inmarsat support site - http://www.inmarsat.com/support

Can the new 176k streaming rate be accessed via the Terminal web interface?
Both Thrane & Thrane and Hughes are working on upgrading their firmware to support 176, Inmarsat will notify the channel once the firmware is available. In the meantime Thrane and Thrane users are able to use the option of creating a new streaming profile, for instructions on how to do this please refer to the thrane manual/user guide.

Is the 176k streaming rate replacing an existing rate?
The new 176k streaming rate is offered as an additional service option, all other streaming services will remain.

Is 176k streaming rate compatible with applications that are set for other rates
As with current BGAN streaming rates, the 176k streaming rate is compatible with leading broadcast video applications. Inmarsat has conducted rigorous testing to ensure that these applications are compatible with the newer streaming rate. Most applications will allow higher or lower rates to be applied however if you are unsure please consult the application user guide for confirmation.

What applications work efficiently with the new 176k Streaming Rate?
Please refer to the Support Tab on the Inmarsat Website where user guides are provided on tested solutions.

How is the 176k streaming rates charged?
Even though this is a new streaming rate, charges are still made on length of time the connection is open as opposed to the amount used. This is in-line with existing streaming rates.

Are there any further expected new streaming rates to be made available?
Currently there are no plans to add any additional streaming rates.

Can I request 176k Streaming if I have 256k Streaming?
If a SIM card is provisioned with Streaming 256K you will be able to request for 176K.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

T&T Explorer 700 shows up as 256k on the LCD and not 176k when requesting 176k

The manufacturer (Thrane) confirm this is correct and a fix will be implemented in the next firmware release which will enable the terminal to be made aware of the new 176k service.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

7| Frequently asked questions about LaunchPad or User Terminal.

7.1| FAQ

Which 'email protocols' can be used with the BGAN service?

Email is usually accessed using four main protocols, all supported on the BGAN network. They are: - POP3 - IMAP4 - Webmail / HTTP - Webmail / SMTP

Why will the terminal not register on the BGAN Network?

The terminal may not have a valid GPS (i.e. the GPS position that is stored may not reflect the user's location, and therefore the terminal must obtain a new GPS). The terminal's signal level may be too low, or the signal may be fluctuating. Problems with low or fluctuating signal can be due to obstructions (e.g. buildings, trees etc) blocking the line of sight to the satellite. Therefore, the initial troubleshooting should involve questioning the user about their local environment.

Is a terminal adapter required for the HUGHES user terminal for ISDN?

Yes, an ISDN Terminal Adapter is required.

How many characters can one SMS typically hold?

From BGAN to any mobile provider, the maximum number of characters that can be contained in one message is 160. Typically, any more than 160 characters will spilt the message in two. This ultimately depends on the type of telephone and the user/recipient's mobile provider. Devices such as the Blackberry and iPhone can hold more characters. It is advised to check with your service and/or telephone provider.

How many contacts and SMS messages can the SIM card hold?

The SIM card can store 100 contacts and 100 SMS messages.

What is the maximum capacity for log files before they are overwritten?

The maximum capacity for a log file is 0.5MB. BGAN uses 3 log files. One for the terminal, and two for 'BGAN LaunchPad' . All log files can only hold a certain amount of information before earlier records are deleted to accommodate new information. It is recommended that important movements are documented at regular intervals, and the log cleared manually to free up space.

Can an external battery charger be used for the Thrane & Thrane User Terminal?

Yes. Solar and car chargers are available from the Local Geoborders Branch (DP) or the manufacturer.

How do I configure routing for User Terminal and multiple devices?

A Traffic Flow Template (TFN) is required (this is a small software file which routes traffic from specific applications across COM ports with specific IP routing options) In addition, the 'BGAN LaunchPad' application provides the option to dedicate streaming connections to certain applications. Information can be found on our website. www.inmarsat.com Please find the direct link below.
www.inmarsat.com/downloads/english/bgan/User_guides/Using_TFTs_on_BGAN

What steps can be taken when BGAN LaunchPad cannot detect the user terminal?

This depends on the type of connection failure. If BGAN LaunchPad cannot detect a terminal a pop-up will appear saying the BGAN terminal cannot detect a terminal. The user will then be given several options to: 1.Perform search again . 2.Define manually how the terminal is connected to the PC or MAC. 3.Cancel and work with BGAN LaunchPad unconnected. 4.Get help connecting to a BGAN terminal. Connection failure can also occur when registering, at this stage there is a pop-up that will appear. This will notify the user that registration is proving difficult and that the network will keep trying.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

What are the user terminal factory restore log-in details?

HNS: Username: None Password: broadband FTP (File Transfer protocol) to HNS user terminal: Username: bgan user Password: broadband T & T: (For factory reset , and to conduct a telnet session on the user terminal) Username: admin Password: 1234 Explorer 100/110: Username: None Password: 9998 Sabre 1: Username: wideye Password: sabre1

How can I determine the static IP (web address) address?

The Thrane terminal can be configured for multi-user mode and the IP displayed will be the external IP (static IP for static IP users.) If your Explorer 700 uses a different IP address, you can look it up by entering the display menu system of the Explorer 700 and selecting PROPERTIES > IP ADDRESS HNS using the Hughes web interface : Click Setup on the menu on the left. This will show the terminal set-up, including the IP address of the terminal. Here IP addresses can also be set. BGAN LaunchPad : Click on View Connection details of terminal. Details of the currently open connections display beneath the connection icons. The displayed details include the Name of the connection, the Owner, the connection Service type, the APN, the IP address, the length of time the connection has been open and the data sent and received.

Does BGAN service support short code access, and in particular short code 33#?

Short codes are compatible with the BGAN service. Please check with your Local Geoborders Branch (DP) for which codes apply to your terminal . Typically 33# will connect the end-user to customer services; however these features are dependent on the Local Geoborders Branch.

What is the factory reset pin for the Wideye Sabre 1 terminal?

Factory reset PIN = 0000

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

7.2| Error Code Descriptions

Error Code CME_3
The root cause is that BGAN LaunchPad has sent a command to the User Terminal that the User Terminal does not recognize and does not respond to. Other likely causes are the User Terminal contains old firmware that does not work with the current LaunchPad version, or the User Terminal has hung and is not able to receive any commands from the BGAN LaunchPad. Re-starting the terminal is recommended. It is also recommended to update firmware (software) to the current version of User Terminal firmware. Then re-start the user terminal.

Error Code CME_4
The root cause is that the LaunchPad has sent a command to the User Terminal that the User Terminal does not recognise and does not respond to. Other likely causes are the User Terminal contains old firmware that does not work with the current LaunchPad version, or the User Terminal has hung and is not able to receive any commands from the LaunchPad. Update User Terminal firmware. Restart the User Terminal.

Error Code CME_5
SIM PIN required. Enter SIM PIN to enable the User Terminal for service.

Error Code CME_10
This indicates that there is no SIM card inserted into the User Terminal. Insert SIM card or contact Local Geoborders Branch (DP) to obtain a SIM card.

Error Code CMS_1
The recipient's number does not exist. Check the number and try again.

Error Code CMS_8
The text messaging service does not work. Contact Local Geoborders Branch (DP) for assistance.

Error Code CMS_10
This indicates that the text messaging service has been barred. Contact Local Geoborders Branch (DP) for assistance.

Error Code CMS_28
The network does not recognise the SIM card. Contact Local Geoborders Branch (DP) for assistance.

Error Code CME_14
The SIM card is busy. It may be in use by another application. Try again later.

Error Code CME_26
This indicates that the number entered is too long. Check the number and try again.

Error Code CMS_30
The SIM card was not recognised by the Network. Contact Local Geoborders Branch (DP) for assistance.

Error Code CMS_50
The subscription for the SIM card does not allow the text messaging facility. Contact Local Geoborders Branch (DP) for assistance.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Error Code CME_27
A letter or symbol has been entered in place of a number. The telephone number can only contain numerical digits. Check the number and redial.

Error Code CME_102
The network does not recognise the SIM card. Contact Local Geoborders Branch (DP) for assistance.

Error Code CME_103
The SIM card has been barred from use. Contact the Local Geoborders Branch (DP) for assistance.

Error Code CME_106
The SIM card has been barred from use. Contact the Local Geoborders Branch (DP) for assistance.

Error Code CME_109
The SIM card details are not recognized by the network. Power down the User Terminal, remove and replace the SIM card, restart the User Terminal and try again.

Error Code CMS_144
This means that the alphabet used in the text message is not recognised by the Network. It is recommended to use a language that is more widely recognised.

Error Code CMS_145
The class of the text message sent is not supported by the Network. Change message class and try again.

Error Code CMS_195
The network cannot detect the telephone number supplied. It is advised to double check the number and try again.

Error Code CMS_196
Sending a text message to a specified number is barred. Contact Local Geoborders Branch (DP) for assistance.

Error Code CMS_198
The chosen validity period for the text message is not supported by the Network. Choose a different period for the validity of the text message and try again. If the text message cannot be delivered during the selected validity period, it will be deleted automatically.

Error Code CMS_208
This indicates that the SIM card memory is full. It is advised to delete text messages that are not required.

Error Code CMS_213
There was an error when downloading SIM data. It is advised to: wait and try again later; reduce the size of data being downloaded. If the problem continues to persist, contact Local Geoborders Branch (DP).

Error Code CMS_310
No SIM card is inserted in the User Terminal. Insert the SIM card and try again.

Error Code CMS_313
The SIM card is faulty. Contact Local Geoborders Branch (DP) for assistance.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Error Code CMS_314
The SIM card is busy. It may be in use by another application. Try again later.

Error Code CME_113
The SIM card is faulty. Contact Local Geoborders Branch (DP) for assistance.

Error Code CME_117
Authentication onto the BGAN Network has failed. This can be due to a number of errors regarding initial authentication. Check with your Local Geoborders Branch (DP) whether the SIM card has been authenticated correctly. It will need to be verified against the Local Geoborders Branch's radius server.

Error Code CME_133
The requested Service is not available within the SIM subscription. Check that the APN (Access Point Name) the customer is requesting has been activated. If the customer is in a 'forced routing' area, check that the applicable 'forced routing' APN has been activated. This can be checked with your Local Geoborders Branch (DP).

Error Code CMS_311
SIM PIN required. Enter SIM PIN to enable the User Terminal for service.

Error Code CME_140
A Secondary Connection has been requested but no traffic template has been configured. Therefore, the Secondary Connection has not been granted. 1. Open a Primary Connection 2. Configure a Traffic Template for the desired Secondary Connection. This can be actioned via BGAN LaunchPad. 3. Once the Traffic Template has been configured , a Secondary Connection can be requested.

Error Code CME_149
The Network needs a correct user name and password to grant the requested service. Associate a correct user name and password with the requested APN and try again.

Error Code CME_150
The type of terminal you are using to connect to the Network is not valid. Contact the Local Geoborders Branch (DP). A User Terminal supporting the BGAN service may be required.

Error Code CME_148
This error code can be displayed when the user is unable to open a data connection as the PDP context has been rejected, or a position response from the terminal has not been received by the Network. The Following steps are recommended: 1. Check that the APN (Access Point Name) the customer is using has been activated. 2. Check that the APN is entered into the LaunchPad correctly. 3. Check that the terminal has a valid GPS, and a strong stable signal.

Error Code CME_152
The User Terminal has no service subscription. The Local Geoborders Branch (DP) will need to activate the SIM card.

Error Code CME_162
This shows that the requested operation is not applicable or not possible. Contact Local Geoborders Branch (DP) for assistance.

Error Code INM_3
The User Terminal is incompatible with the BGAN network (radio interface). Contact Local Geoborders Branch (DP) for assistance.

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

8| How to Upgrade the Firmware of your Device.

You can download all updated Firmware and Installation Guides at the on-line portal for Geoborders Customers at the website www.geoborders.com in the Section **Help & Support.**

Note: GEOBORDERS recommend that all INMARSAT Customers run latest versions of firmware on their terminals, as soon as become available.

9| Download your terminal User Guides

You can download this user guide and all updated manuals and Best Practice Guides at the on-line portal for Geoborders Customers at the website www.geoborders.com in the Section **Help & Support**

10| Register on-line your Terminal for Warranty

You can register your satellite phone or device at **My Geoborders**, the on-line portal for Geoborders Customers at the website www.geoborders.com

11| How to Activate your SIM Card

You can activate your SIM Card ONLINE going to www.geoborders.com/activation/ and follow the attached instructions, fill it up with all your personal or company details, choose your Airtime Plan, add the SIM Card or your device Serial number.
You are also required to send your Photo Id to: activations@geoborders.com

12| Appendix

12.1| Customer Care Contacts

You can contact GEOBORDERS Customer Care at the **toll-free number +800.3333.6666**, this number is operative almost all over the world. If you cannot reach this number please call **+44.186.55.760.22** In some countries or through some satellite equipment you will have to dial "00" instead of "+" so numbers will become:

+800.3333.6666
00800.3333.6666
(Worldwide Toll-free in 61 countries)

+44.(0)20.3051.3846
(From Satellite Phone and Countries where Toll free is not available)

support@geoborders.com

12.2|On-line Customer Service

You can contact reach GEOBORDERS Customer Service at the website www.geoborders.com and follow on-line instructions.

12.3|Registered Trademarks

12.4|Limitation of Liability

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

Web Sites for your reference:

www.inmarsat.com
(Inmarsat Plc official web site)

www.inmarsat.com/support
(technical support and Firmware download)

www.geoborders.com
(Service Provider)

First Edition: March 2008
Last Edition: November 2012

Last Printed: November 2012

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com

NOTES

GEOBORDERS SATELLITE
Tel: +44.(0)20.3051.3846
Toll Free: +800.3333.6666 (open 24/24 hours)
E: support@geoborders.com