



FleetBroadband Best Practices Manual

Version 1.0
January 2009

inmarsat.com/fleetbroadband

Whilst the information has been prepared by Inmarsat in good faith, and all reasonable efforts have been made to ensure its accuracy, Inmarsat makes no warranty or representation as to the accuracy, completeness or fitness for purpose or use of the information. Inmarsat shall not be liable for any loss or damage of any kind, including indirect or consequential loss, arising from use of the information and all warranties and conditions, whether express or implied by statute, common law or otherwise, are hereby excluded to the extent permitted by English law. INMARSAT is a trademark of the International Mobile Satellite Organisation, Inmarsat LOGO is a trademark of Inmarsat (IP) Company Limited. Both trademarks are licensed to Inmarsat Global Limited. © Inmarsat Global Limited 2008. All rights reserved.

Contents

1. Introduction.....	1
1.1 Purpose of document.....	1
1.2 Audience	1
2. FleetBroadband Overview	1
2.1 FleetBroadband In-orbit Infrastructure	1
2.2 FleetBroadband Terrestrial Infrastructure.....	2
2.2.1 <i>Satellite Access Stations (SAS)</i>	2
2.2.2 <i>Regional Hubs or Points of Presence (PoPs)</i>	2
2.2.3 <i>Network Operations Centre (NOC)</i>	2
2.2.4 <i>Satellite Control Centre (SCC)</i>	2
2.2.5 <i>Business Support Services (BSS)</i>	3
2.3 FleetBroadband Services	3
2.4 One Device, Two Domains, Three Data Networks	3
2.4.1 <i>Standard IP Data</i>	4
2.4.2 <i>Streaming IP Data</i>	4
2.4.3 <i>Circuit-switched Data Services</i>	5
2.5 Voice and Messaging Services	6
2.5.1 <i>Direct Dial Voice Service</i>	6
2.5.2 <i>Voicemail Service</i>	6
2.5.3 <i>Global Text</i>	7
2.6 Product Types	7
2.7 FleetBroadband Dynamic Network Management	9
2.8 FleetBroadband Performance Factors.....	9
2.8.1 <i>Key Elements of the FleetBroadband System</i>	9
2.8.2 <i>Vessel Equipment</i>	10
2.8.3 <i>Satellite Interconnect</i>	10
2.8.4 <i>Distribution Partner - PoP Interconnect</i>	10
2.8.5 <i>User Interconnect/General Internet Access</i>	10
2.9 FleetBroadband Benefits Summary	10
3. Pre-Installation Planning - Vessel	11
3.1 Different Terminal Features and Configurations.....	11
3.2 Terminal Installation.....	12
3.2.1 <i>Overview</i>	12
3.2.2 <i>Equipment location</i>	12
3.2.3 <i>Hotworks</i>	13
3.2.4 <i>Antenna Cabling</i>	13
3.2.5 <i>IP Network Cabling, WiFi and Voice/Fax/Data Port Locations</i>	14
3.2.6 <i>Power</i>	14
3.2.7 <i>Fast Installation without downtime</i>	14
4. Pre-Installation Planning – HQ	14

4.1	Connecting to your Distribution Partner – the “Last Mile”	14
4.2	Internet-based Last-Mile solutions for use with a Standard IP connection .	15
4.3	Guaranteed Last-Mile solutions for use with a Streaming IP connection ...	16
4.4	Distribution Partner (DP) Infrastructure Considerations	16
4.5	VPN Implementation	17
4.6	Corporate Intranet Design Considerations.....	18
4.7	Implementation Notes for Corporate Enterprise Systems	18
5.	Vessel Network Considerations	18
5.1	Typical Vessel Communications Network	18
5.2	Integration with existing communications infrastructure	19
5.3	Integration of other subsystems on board	19
5.4	Ethernet options/sub-networks.....	20
5.5	Selecting an IP connection type.....	20
5.5.1	<i>Standard IP</i>	21
5.5.2	<i>Streaming IP</i>	21
5.5.3	<i>Dedicated Streaming IP</i>	22
5.5.4	<i>Which IP connection should I use?</i>	23
5.6	TCP/IP and UDP/IP	25
5.6.1	<i>About TCP/IP</i>	25
5.6.2	<i>About UDP/IP</i>	25
5.7	LaunchPad, Web Interface and AT commands	26
5.7.1	<i>LaunchPad</i>	26
5.7.2	<i>Web Interface</i>	26
5.7.3	<i>AT Commands</i>	27
5.8	Traffic Flow Template (TFT)	28
5.9	Security Settings and Related Value Added Services.....	28
5.9.1	<i>Firewall</i>	28
5.9.2	<i>Proxy Server</i>	28
5.9.3	<i>MAC address management/control</i>	28
5.9.4	<i>DDNS (dynamic domain name server) updating</i>	28
5.9.5	<i>External Router</i>	29
5.9.6	<i>DP Filtering</i>	29
6.	Optimising IP settings.....	29
6.1	Satellite Latency and Jitter	29
6.2	TCP Window Size.....	30
6.3	MTU, MSS and RWIN	31
6.3.1	<i>MTU (Maximum Transmission Unit)</i>	31
6.3.2	<i>MSS (Maximum Segment Size)</i>	31
6.3.3	<i>RWIN</i>	31
6.4	Quiescent Mode	32
6.5	TCP/IP Slow Start.....	32

6.5.1	<i>TCP Slow Start Overview</i>	32
6.5.2	<i>FTP Slow Start</i>	33
6.5.3	<i>HTTP (Web Browsing) Slow Start</i>	33
6.6	TCP Accelerator (TCP PEP).....	34
6.6.1	<i>About TCP Accelerator</i>	34
6.6.2	<i>TCP Accelerator Solutions</i>	34
7.	Connecting Peripheral Devices to the FleetBroadband Terminal	35
7.1	DHCP - Address allocation.....	35
7.2	Network Address Translation (NAT) Mode	36
7.3	Modem Mode.....	36
7.4	Port Forwarding	37
7.5	IP Connections Explained.....	37
7.5.1	<i>About PDP contexts</i>	37
7.5.2	<i>FleetBroadband and PDP contexts</i>	38
7.5.4	<i>How static IP addressing is provisioned</i>	39
8.	Maintenance, Support and Security Procedures	39
8.1	Training and Handover	39
8.2	Remote Support	39
8.3	Error Logging.....	40
8.4	Useful IP tools.....	40
8.5	Standby PC and Ghost Images.....	40
8.6	Operational procedures	41
8.7	Access control.....	41
8.7.1	<i>User levels</i>	41
8.7.2	<i>Web access rules</i>	41
8.7.3	<i>Pre-emption in case of emergencies</i>	41
8.7.4	<i>BIOS and Desktop Locks</i>	41
8.8	Scheduling.....	42
8.9	Ship-to-shore Liaison and Escalation procedures.....	42
9.	Communication Cost Management	42
9.1	Develop a traffic profile.....	42
9.2	Least-cost Routing - Manual and Automatic	43
9.3	Traffic Monitoring Tools	43
9.3.1	<i>DP Solutions</i>	44
9.3.2	<i>Third-party Solutions</i>	44
9.4	Automatic Updates.....	44
9.5	Domain Name Server (DNS) Traffic	45
9.6	Using Web-caching.....	46
9.7	Reducing Unnecessary LAN Traffic	46
9.7.1	<i>Block unwanted traffic</i>	46
9.7.2	<i>Polling/update checks</i>	46

10. Applications Optimisation.....	47
10.1 Voice/VoIP	47
10.2 Fax.....	47
10.3 Chat	47
10.4 Email.....	47
10.4.1 <i>Improving email performance</i>	47
10.4.2 <i>Optimising email clients</i>	48
10.4.3 <i>Optimising Outlook Express</i>	48
10.4.4 <i>Optimising Eudora 5.1</i>	49
10.4.5 <i>Optimising Mozilla Thunderbird</i>	50
10.4.6 <i>Using specialised email solutions</i>	50
10.4.7 <i>Web-mail</i>	51
10.5 Web browsing	51
10.5.1 <i>Middleware</i>	51
10.5.2 <i>Structured Browsing</i>	52
10.5.3 <i>Web Browser Optimisations</i>	52
11. Operating System Optimisation	53
11.1 Windows OS Optimisations.....	53
11.2 Linux OS Optimisations	54
11.3 Mac OS Optimisations.....	55
12. How can you benefit from FleetBroadband?	56
12.1 Maritime Industry Trends	56
12.2 Ship Management Functions & Responsibilities.....	56
12.3 Cost-Effective Ship Operations	57
12.4 Crew Welfare and Retention.....	58
12.4.1 <i>Crew Calling</i>	58
12.4.2 <i>Crew Email and Internet Access</i>	59
12.5 Reduced fuel costs	59
12.5.1 <i>Weather Routing</i>	60
12.5.2 <i>Engine Maintenance (Preventative and Predictive)</i>	60
12.6 Imaging and Video Applications	60
12.6.1 <i>Maritime Imaging and Video Applications</i>	60
12.6.2 <i>Digital Photos</i>	60
12.6.3 <i>Video Chatting</i>	60
12.6.4 <i>Store & Forward Video</i>	61
12.6.5 <i>Video Streaming</i>	61
12.6.6 <i>Video conferencing</i>	61
12.7 Ship Management Applications	61
12.8 Fishing Applications	61
12.8.1 <i>Geoeye</i>	61
12.8.2 <i>Catsat</i>	61

12.8.3 *PEFA*..... 62
12.8.4 *Maxsea*..... 62
12.8.5 *Traceall*..... 62
12.8.6 *Tracefish*..... 62

1. Introduction

1.1 Purpose of document

This document has been written for owners, managers and crews of vessels equipped with, or about to be equipped with, the Inmarsat FleetBroadband system.

It is intended to provide guidance and best practice recommendations on key elements of the deployment, integration and use of the FleetBroadband system to ensure that the maximum benefits are realised from the system in the most cost-effective manner.

Many of the recommendations contained herein are based on actual experience and lessons learned from the FleetBroadband Maritime Field Evaluation trials recently carried out by Inmarsat on ten FleetBroadband-equipped vessels worldwide.

1.2 Audience

Marine superintendents, IT deployment managers and Distribution Partner and Service Provider channel sales executives.

2. FleetBroadband Overview

2.1 FleetBroadband In-orbit Infrastructure

FleetBroadband 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.

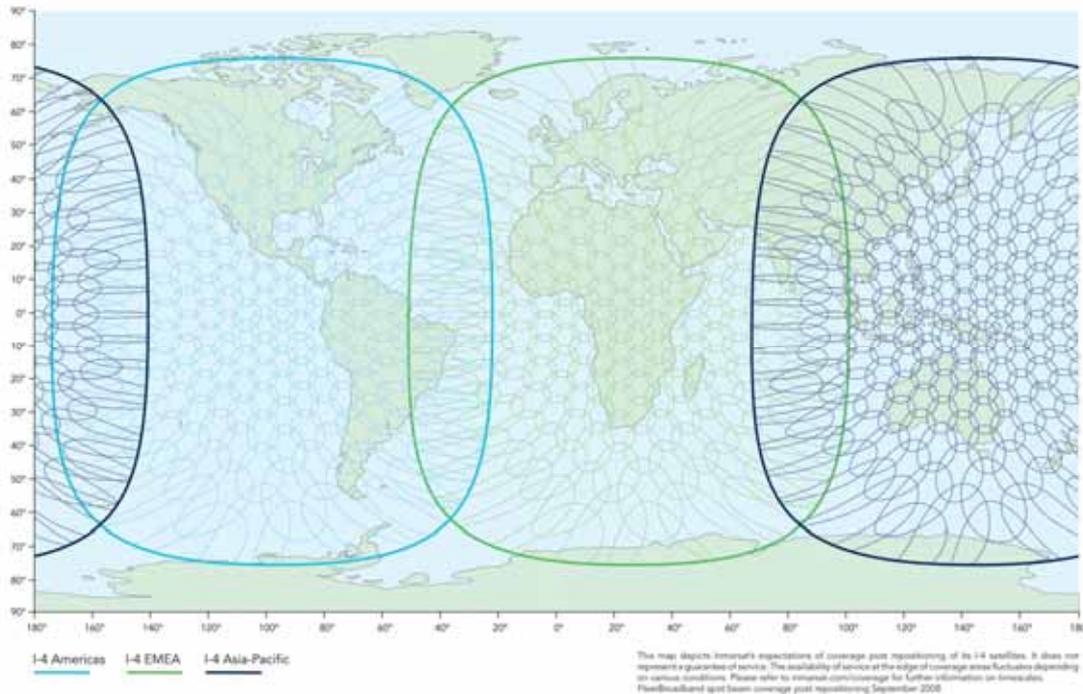


Figure 1 Inmarsat 4 Global Coverage (as at 18th Feb 2009)

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.

2.2 FleetBroadband Terrestrial Infrastructure

The in-orbit infrastructure is complemented by the FleetBroadband terrestrial infrastructure which comprises five principle elements as shown below in Figure 2 and as described in the following sections.

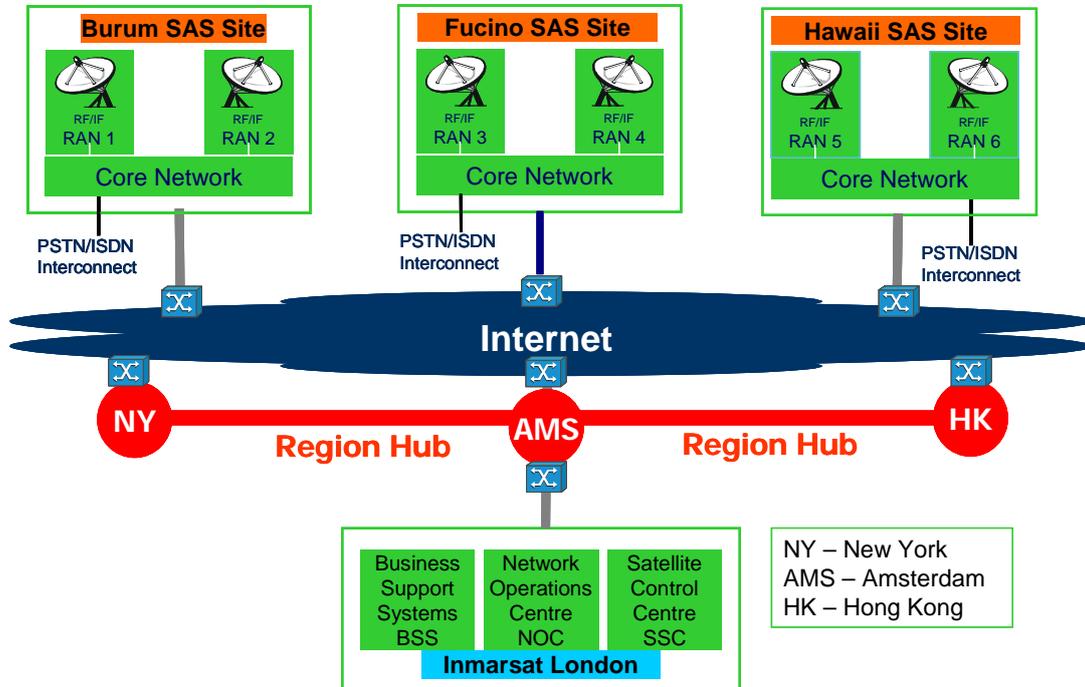


Figure 2 FleetBroadband Terrestrial Infrastructure

2.2.1 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.

2.2.2 Regional Hubs or Points of Presence (PoPs)

The Regional Hubs (or PoPs) are the gateway to the Inmarsat FleetBroadband 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 Inmarsat Distribution Partners, access to the Meet Me Points can also be provided for end-users by arrangement with your Distribution Partner.

The regional hubs are owned and operated by third parties on behalf of Inmarsat and are currently operated by Telx in New York, Telecify in Amsterdam and HKCOLO in Hong Kong.

2.2.3 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 FleetBroadband network worldwide.

2.2.4 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.

2.2.5 Business Support Services (BSS)

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

2.3 FleetBroadband Services

FleetBroadband 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!

	<p>Voice</p>	<ul style="list-style-type: none"> • 4kbps circuit-switched service • Voicemail • Enhanced services: call waiting, forwarding, barring, holding • Broadcast quality voice
	<p>Data Standard IP</p>	<ul style="list-style-type: none"> • High Speed Standard IP (NOT MPDS) • Variable bit rate service – Shared & Best Effort • Up to 432/432 kbps (send /receive)
	<p>Data Streaming IP</p>	<ul style="list-style-type: none"> • On-demand guaranteed bit rate service • 32, 64, 128, 256 kbps (send & receive) (ISDN legacy compatibility)
	<p>Global Text</p>	<ul style="list-style-type: none"> • Send and receive text messages via your laptop

Figure 3 Inmarsat FleetBroadband Services

2.4 One Device, Two Domains, Three Data Networks

FleetBroadband 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 FleetBroadband 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.

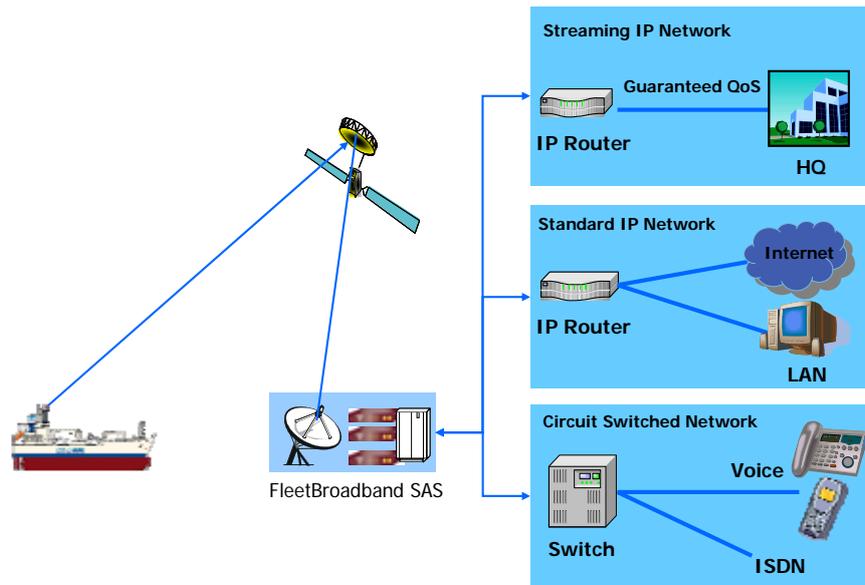


Figure 4 One Device, Two Domains, Three Data Networks

2.4.1 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 FleetBroadband 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.

2.4.2 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.

FleetBroadband 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 capacity is delivered in both the forward and return directions and a streaming connection has a per minute tariff structure.

2.4.3 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 FleetBroadband network supports mobile-originated and mobile-terminated ISDN circuit-switched data calls at 64kbps.

FleetBroadband 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, FleetBroadband 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 FleetBroadband terminal types. Table 1 below, entitled FleetBroadband Circuit-Switched Data Services by Terminal Type summarises the different circuit-switched data services available on the different FleetBroadband types.

Terminal Type	ISDN	3.1kHz Audio
FleetBroadband 500	✓	✓
FleetBroadband 250	×	✓
FleetBroadband 150	×	×

Table 1 FleetBroadband Circuit-Switched Data Services by Terminal Type

Note:

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

¹ Class 8 only

² Service not supported below 20 degrees elevation on Class 9 (FB 150 and FB250)

2.5 Voice and Messaging Services

2.5.1 Direct Dial Voice Service

FleetBroadband 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 FleetBroadband terminals
- Landline quality speech (voice encoded at 4kbps)
- To and from
 - Terrestrial networks
 - Mobile networks
 - FleetBroadband terminal to FleetBroadband 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 FleetBroadband 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 2 FleetBroadband Generic Short-codes

2.5.2 Voicemail Service

FleetBroadband 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

³ The AMBE+2 audio codec was developed by DSVI Inc. and is a toll-quality, full-duplex, real-time voice compression software.

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 FleetBroadband network (57) or by dialling + 00 870 77200 1899 from any other network.

2.5.3 Global Text

The FleetBroadband network incorporates an SMS (text) messaging application with a full range of messaging features. The SMS message format follows the standard 160 character structure. FleetBroadband does not support concatenated SMS.

You can send and receive SMS messages to and from other FleetBroadband terminals and terrestrial cellular networks⁴ via your laptop or computer using the FleetBroadband LaunchPad utility as shown below in Figure 5.

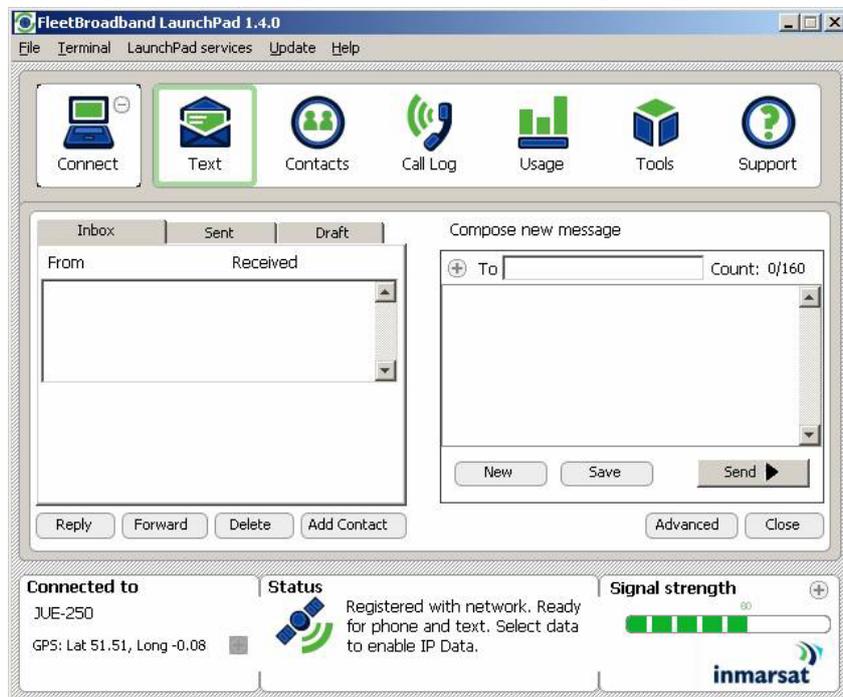


Figure 5 LaunchPad SMS (Text) Interface

2.6 Product Types

There are two terminal types defined and type-approved for the FleetBroadband service. They are referred to as Class 8 (High Gain Antenna “FB500”) and Class 9 (Low Gain Antenna “FB250” and “FB 150”) terminals. The key difference between Class 8 and Class 9 is the antenna.

For each type of FleetBroadband terminal Inmarsat defines:-

⁴ Subject to roaming agreements – please check with Inmarsat Customer Care for the most up to date list of cellular roaming partners.

1. the air interface at the output of the terminal’s antenna;
2. the mandatory features and service types for each class of user terminal; and,
3. the performance requirements of the user terminal.

Manufacturers must meet all of these requirements in order to obtain Type Approval.

The definition of other equipment features such as physical connections, user interfaces, firewalling, routing control etc is determined by each manufacturer according to specific market-driven needs. Because of the possibility of different physical interfaces on terminals from different manufacturers users should pay particular attention to the installation guidelines given in Section 3.1 of this manual, entitled Different Terminal Features and Configurations.

A summary of the features of each of the FleetBroadband terminals is shown below in Table 3, entitled Summary of FleetBroadband Terminal Features.

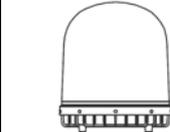
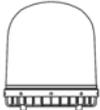
Hardware Definition	FleetBroadband 500 (Class 8 High Gain)	FleetBroadband 250 (Class 9 Low Gain)	FleetBroadband 150 (Class 9 Low Gain)
Radome View (as per F55, mini-M)			
Antenna Diameter	~ 55cm	~ 25cm	tbd
Antenna G/T (at 5° elevation)	-7 dB/K	-15 dB/K	-15 dB/K
Antenna EIRP	22 dBW	15.1 dBW	15.1 dBW
Antenna type	Directional/3-axis stabilised	Directional/3-axis stabilised	tbd
Antenna target weight	15 - 20 kg	3 – 5 kg	tbd
Voice (Simultaneous with data)	4kbps	4kbps	4kbps
Contended Standard IP Tx/Rx kbps (shared/best efforts)	Up to 432/432 kbps	Up to 239/284 kbps	Up to 150 kbps
ISDN	Yes	3.1Khz audio only	None
I.P. ‘Streaming Mode’ Guaranteed Throughput, kbps	32, 64, 128 & 256	32, 64, 128	None
Upgrade Path ⁵	JRC confirmed F77 (ADU)	JRC confirmed F33 (ADU)	None
Physical Interfaces/Ports	RJ11, Ethernet, RJ45 (ISDN), L-band RF	RJ11, Ethernet, RJ45 (ISDN), L-band RF	RJ11, Ethernet

Table 3 Summary of FleetBroadband Terminal Features

⁵ Please confirm availability with manufacturer.

2.7 FleetBroadband Dynamic Network Management

FleetBroadband Standard IP data is a variable bit-rate service provided on a shared or contended channel and operating up to 432kbps (FleetBroadband 500) in each direction on a best efforts basis.

Inmarsat manages this service by dynamically allocating satellite resources to the Standard IP data service to ensure that users experience the best possible performance.

Factors taken into account in managing this service include:-

- Total volume of traffic (and not just the activity in the channel)
- Number of users in the spot beam
- The level of activity in other spot beams
- Spare channels available
- Forecast use based on historical data
- Overall number of users
- Average bandwidth currently experienced
- How long has this pattern of heavy use been prevalent

Thus Inmarsat is able to dynamically and transparently provide additional satellite resources to vessels demanding more capacity and restore and re-allocate those resources when that demand has been satisfied.

2.8 FleetBroadband Performance Factors

2.8.1 Key Elements of the FleetBroadband System

The FleetBroadband system is made up of several elements, as illustrated below in Figure 6, entitled FleetBroadband End-to-End System Diagram, all of which need to be optimised to enhance your experience as a user.

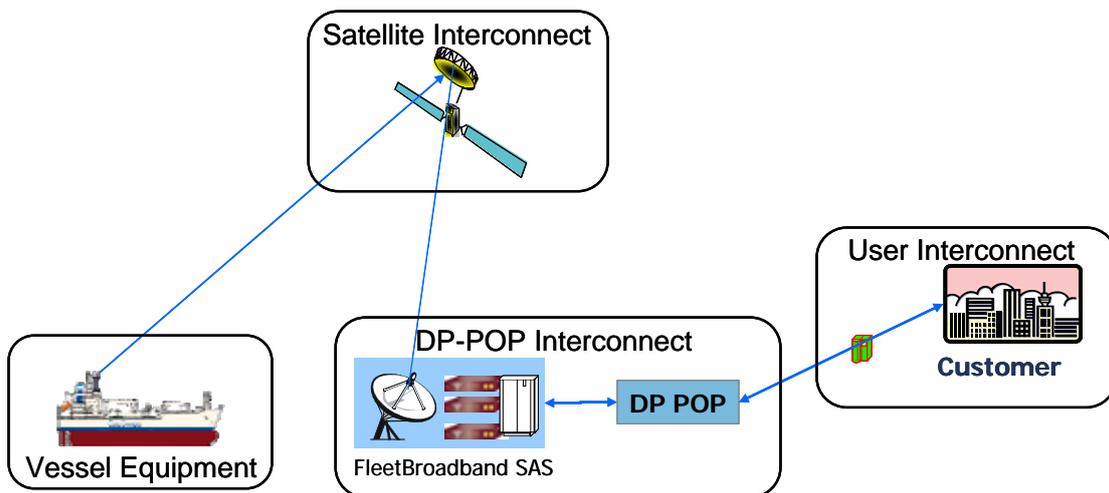


Figure 6 FleetBroadband End-to-End System Diagram

All of these components and parameters are discussed in this manual together with optimisations recommended by Inmarsat to ensure that you obtain the best possible performance from your FleetBroadband system.

The four key elements shown above in Figure 6 are discussed in the following

paragraphs.

2.8.2 Vessel Equipment

The equipment and configuration installed on the vessel is the responsibility of the Customer but it is expected that guidance will be provided by the Inmarsat Distribution Partner or Service Provider. Primary consideration should be given to:

- Onboard computers, hardware and operating system (e.g. Windows, MAC, Linux) including:-
 - User applications/protocols – FTP, IMAP, POP, SMTP, HTTP
 - Transport protocol – TCP/IP or UDP
- Appropriate optimisation of applications and communications software
- Wiring and Ethernet connectivity
- Terminal installation and in particular the location of the antenna

2.8.3 Satellite Interconnect

The satellite interconnect is generally transparent to a user. However, in some circumstances (troubleshooting, optimisation etc), it may be necessary to consider the following factors in conjunction with your Distribution Partner:-

- Optimal satellite selection
- Dynamic Network Management
- Satellite Access Gateway
- Latency and jitter – round trip time
- Network activity – network resources

2.8.4 Distribution Partner - PoP Interconnect

User traffic is routed through the DP PoP for onward transmission and the provision of value-added services such as DNS IP addressing, billing management, security, firewalling and provision of a dedicated “last-mile” connection if required by the Customer. The DP – PoP interconnect is the DP’s responsibility

2.8.5 User Interconnect/General Internet Access

The final routing of a user’s traffic from the PoP to its ultimate destination (general Internet access or to the customer’s own infrastructure) is the responsibility of the customer and the routing selected will determine the QoS that a user’s traffic will experience. If a high Quality of Service is required then a dedicated connection should be considered otherwise Internet-based routing may be sufficient.

The routing, and hence type of connection implemented, will be determined by the nature of the FleetBroadband services to be used and the required Quality of Service. This is discussed further in Section 4.1 below, entitled Connecting to your Distribution Partner – the “Last Mile”.

Your DP will advise you on the routing and type of connection most suited to your traffic.

2.9 FleetBroadband Benefits Summary

In addition to the proven Inmarsat heritage and L-band characteristics which include:-

- Unaffected by the weather – operates in rain, heavy cloud cover, and storms
- Licensed to work in ANY territorial waters – no regulatory constraints

- Powerful global service
- Completely dependable, even in the toughest sea conditions
- A field-proven history of integrated, reliable products and service

FleetBroadband has the following unique selling features:-

- Higher bandwidth
- Crystal-clear voice
- Simultaneous voice and data
- Common user interface for easy set-up and use
- Compact antennas for easy installation and maintenance
- Range of flexible and affordable rate plans
- Unprecedented data speeds available globally for maritime users

These features are further enhanced by a wide range of sophisticated Value Added Services and solutions available from the Inmarsat Distribution Partners such as those listed in Section 4.4 below.

3. Pre-Installation Planning - Vessel

3.1 Different Terminal Features and Configurations

All of the FleetBroadband terminals provide all of the services described above in Section 2.3 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 FleetBroadband 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. Some examples of popular FleetBroadband terminal physical interface options are shown below in Figure 7 and Figure 8.

Further information on connecting peripheral devices to your FleetBroadband system is given in Section 5 below, entitled Vessel Network Considerations



Figure 7 Thrane & Thrane Physical Interfaces

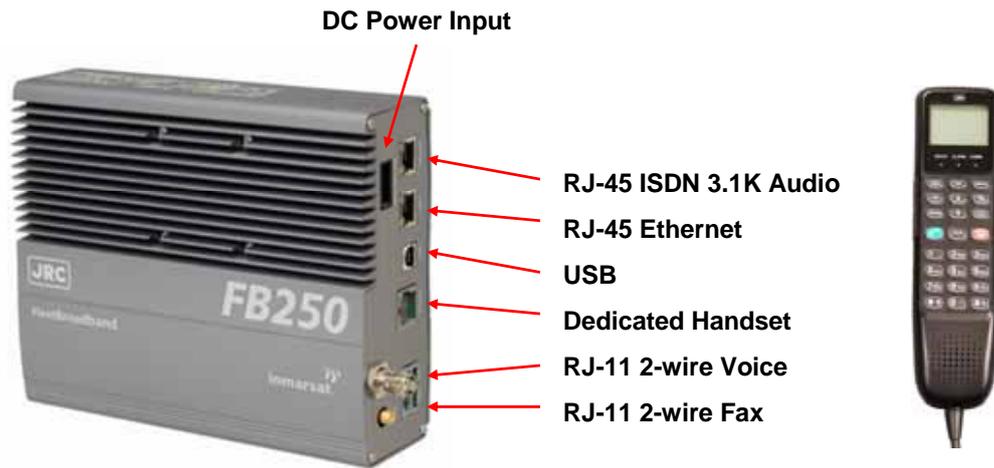


Figure 8 JRC FleetBroadband 250 Physical Interfaces

3.2 Terminal Installation

3.2.1 Overview

FleetBroadband 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.

3.2.2 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.

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.

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.

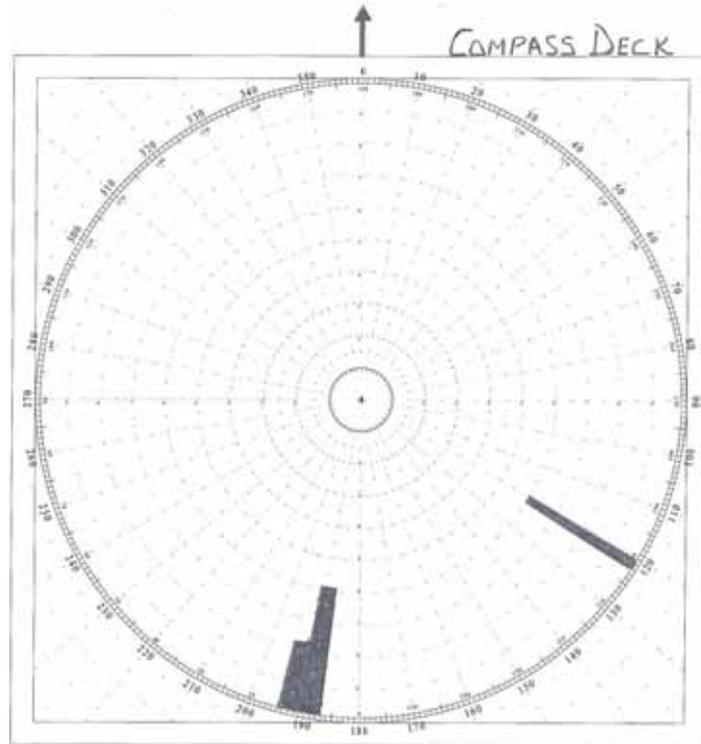


Figure 9 Example Shadow Area Chart

3.2.3 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.

3.2.4 Antenna Cabling

The FleetBroadband 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
RG214 - FRNC	12 m	50 m
S10162B11	30 m	100 m
RG ½" 50	45 m	100 m

Table 4 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.

3.2.5 IP Network Cabling, WiFi and Voice/Fax/Data Port Locations

You should consider where the FleetBroadband Below Decks Equipment (BDE) is 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 FleetBroadband 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.

3.2.6 Power

FleetBroadband 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 FleetBroadband BDE and associated network equipment and peripherals devices.

3.2.7 Fast Installation without downtime

The FleetBroadband 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.

4. Pre-Installation Planning – HQ

4.1 Connecting to your Distribution Partner – the “Last Mile”

Inmarsat manages the Quality of Service (QoS) within the FleetBroadband network, QoS being defined by various parameters including bit-rate, latency, jitter and packet loss. When a FleetBroadband data connection is opened, the QoS for the connection is negotiated between the FleetBroadband terminal and the FleetBroadband 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 Distribution Partner or Service Provider and your corporate network, often referred to as the “last mile”, needs to be commensurate with the type of FleetBroadband 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 FleetBroadband 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 FleetBroadband connection for your applications you should then choose the appropriate last-mile interconnect.

Your FleetBroadband 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).

4.2 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.

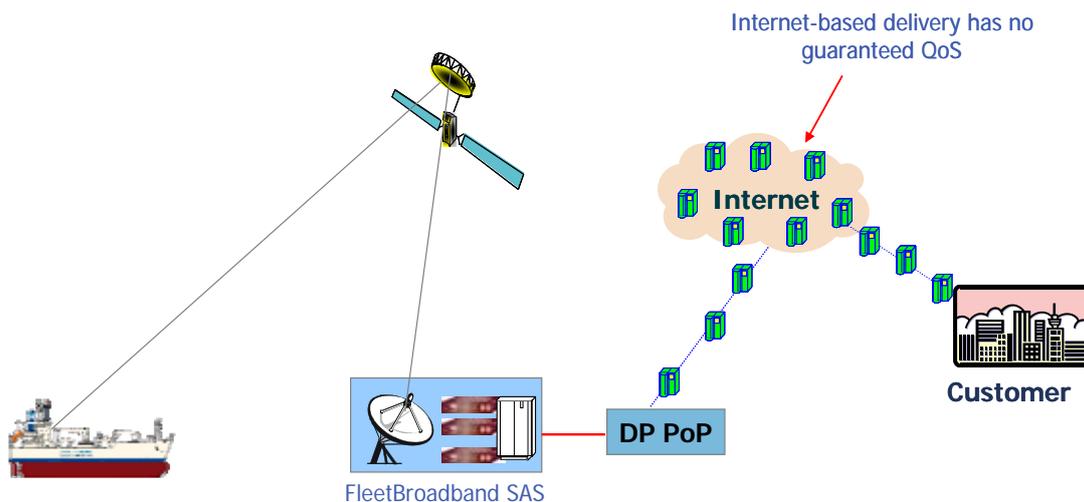


Figure 10 Internet-based Last Mile Implementation

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)

4.3 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.

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.

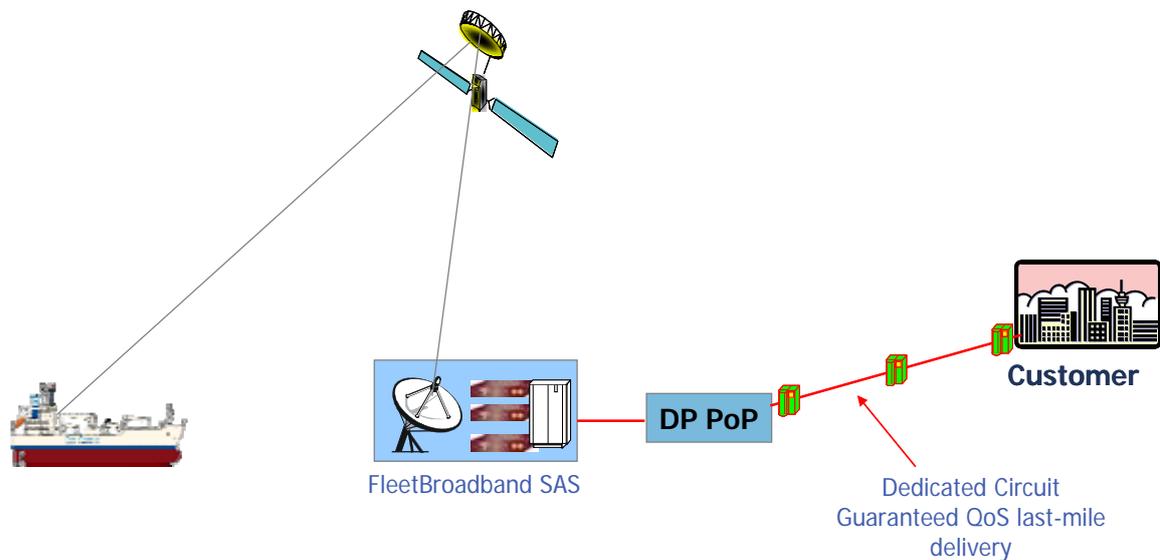


Figure 11 Dedicated Circuit Guaranteed QoS Last Mile Implementation

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

4.4 Distribution Partner (DP) Infrastructure Considerations

Have you selected your Inmarsat Distribution Partner 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

Some of the features you may need from your Distribution Partner 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

4.5 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 FleetBroadband. Such an approach would be quite workable and most commercially available VPN implementations will operate seamlessly over FleetBroadband.

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 FleetBroadband 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 FleetBroadband network.

4.6 Corporate Intranet Design Considerations

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

4.7 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 “lite” and therefore not usually “mobile friendly”.

If such a system is to be used in conjunction with the FleetBroadband 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

5. Vessel Network Considerations

5.1 Typical Vessel Communications Network

FleetBroadband 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.

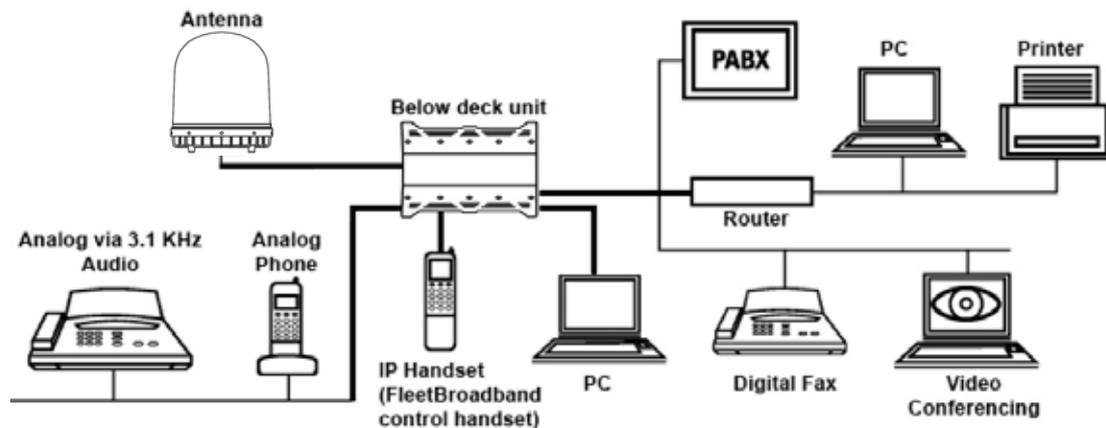


Figure 12 Typical Vessel Communications Network

5.2 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 FleetBroadband terminal are:-

- Handsets: Analogue, Cordless, DECT, ISDN
- Wireless WiFi network
- VoIP Peripherals: USB, WiFi 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 FleetBroadband 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

5.3 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 FleetBroadband 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

5.4 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.

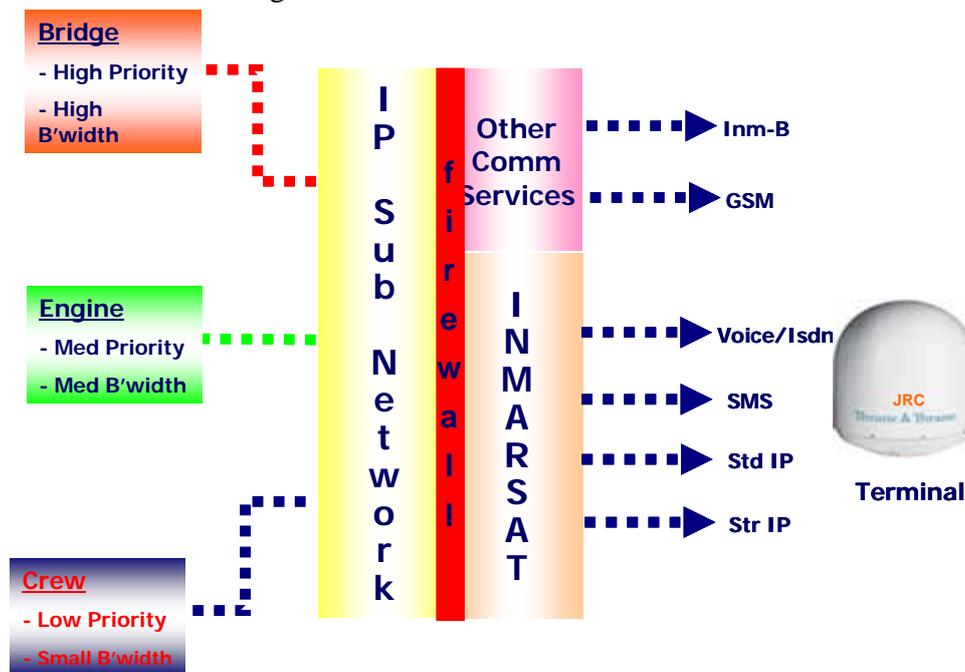


Figure 13 Example of Vessel Sub-Network Implementation

5.5 Selecting an IP connection type

FleetBroadband 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 FleetBroadband terminal for information on opening and closing an IP data connection.

5.5.1 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 FleetBroadband terminal and opens automatically when the terminal is connected to the FleetBroadband 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 FleetBroadband Service Provider for details on how you are charged for a Standard IP connection.

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).

5.5.2 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 Distribution Partner or Service Provider.

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 FleetBroadband LaunchPad settings for that connection

It is possible to configure Streaming IP data connections on the FleetBroadband 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 FleetBroadband 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.

5.5.3 Dedicated Streaming IP

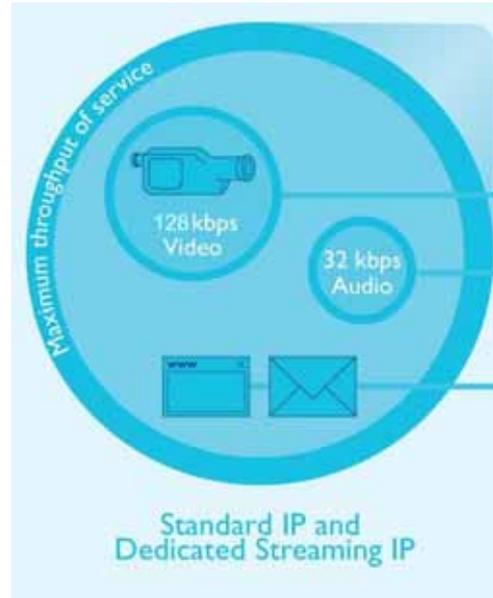
A dedicated Streaming IP connection enables the creation of multiple connections – each of which can be “dedicated” to selected individual applications that need to run simultaneously. By using port forwarding (see Section 7.4 below) it is possible to “route” these dedicated connections to multiple devices 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 FleetBroadband 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 FleetBroadband terminal and FleetBroadband network to work together to “route” these multiple connections successfully a Traffic Flow Template (TFT), also called an Application Template, is used. In the FleetBroadband 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.

5.5.4 Which IP connection should I use?

You can maximise throughput and performance and minimise your traffic costs by selecting the FleetBroadband 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 FleetBroadband, 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	FleetBroadband IP connection type	Further details
------------------	-----------------------------------	-----------------

Application type	FleetBroadband 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	FleetBroadband 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 FleetBroadband 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 FleetBroadband 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 FleetBroadband.
Live Broadcast	256 kbps Streaming IP	FleetBroadband 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	FleetBroadband 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 5 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.

5.6 TCP/IP and UDP/IP

This section gives recommendations for the use of applications using TCP/IP or UDP/IP over the FleetBroadband 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.

5.6.1 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 FleetBroadband 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 FleetBroadband link has the capacity to forward them to their destination. This may cause a further 10% reduction in throughput.

5.6.2 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 FleetBroadband 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.

5.7 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 FleetBroadband. LaunchPad provides the following features:-

- Familiar and simple access for the full range of FleetBroadband 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 14 FleetBroadband LaunchPad Home Screen

5.7.2 Web Interface

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

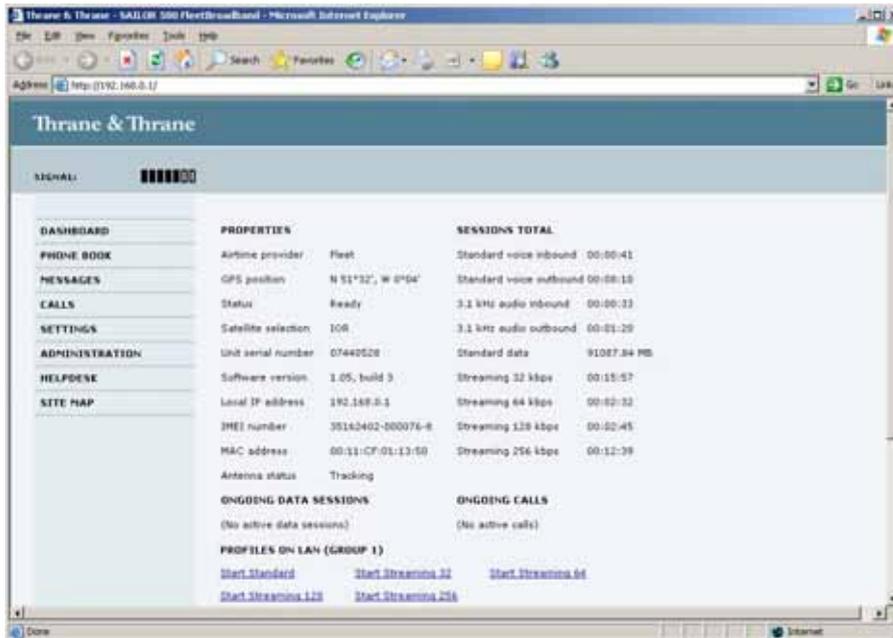


Figure 15 Thrane & Thrane FleetBroadband 500 Web-based Interface

5.7.3 AT Commands

FleetBroadband 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. DHCP 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 5454
JRC	192.168.128.100 1829

Table 6 AT Command Interface

Some typical FleetBroadband 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=1,1,256,256,256,25 6,1500,E30, E40	Set the QoS parameters for a Streaming IP connection

Table 7 Typical FleetBroadband AT Commands

5.8 Traffic Flow Template (TFT)

Traffic Flow Templates are used whenever multiple dedicated Streaming IP 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 FleetBroadband LaunchPad. Users can modify these for their own applications, for example videoconferencing or VoIP.

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

5.9 Security Settings and Related Value Added Services

5.9.1 Firewall

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

5.9.2 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.

5.9.3 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.

5.9.4 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.

5.9.5 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 FleetBroadband:-

- Netgear
- D-Link
- Cisco
- US Robotics

5.9.6 DP Filtering

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

6. Optimising IP settings

This section explains how to optimise IP to get the best possible performance and cost savings over FleetBroadband. 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 FleetBroadband 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.

6.1 Satellite Latency and Jitter

Latency in the FleetBroadband 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 FleetBroadband 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 FleetBroadband 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.

Latency can have a critical effect on the performance of many applications and on the overall user experience and is particularly critical for video applications. 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.

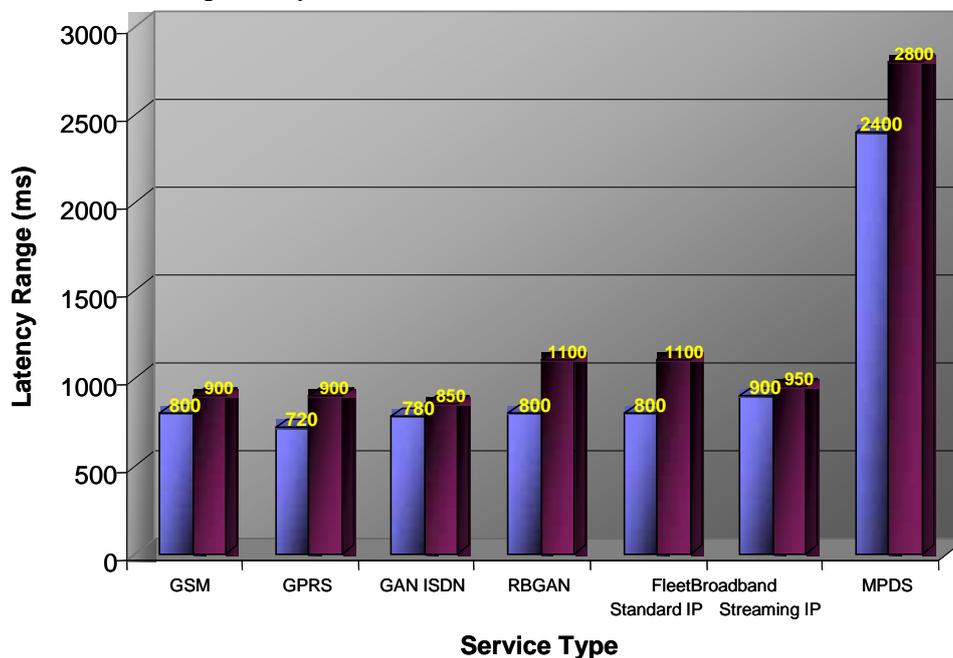


Figure 16 Latency in Communications Networks

6.2 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 FleetBroadband as data loss results in retransmission and additional costs.

TCP window size is also important for the FleetBroadband 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 FleetBroadband.

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.

6.3 MTU, MSS and RWIN

6.3.1 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>

6.3.2 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.

6.3.3 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 FleetBroadband?
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 8 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/drtcp>

6.4 Quiescent Mode

This section applies to Standard IP only.

When you use applications that send or receive data in bursts, the FleetBroadband resourcing algorithm introduces delays. These occur when a connected FleetBroadband 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 FleetBroadband 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.

Applications that are interactive (i.e. requiring constant user interaction) will be affected by this behaviour and every effort should be made to minimise its effect by the use of spoofing or TCP-PEP.

6.5 TCP/IP Slow Start

6.5.1 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 17.

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).

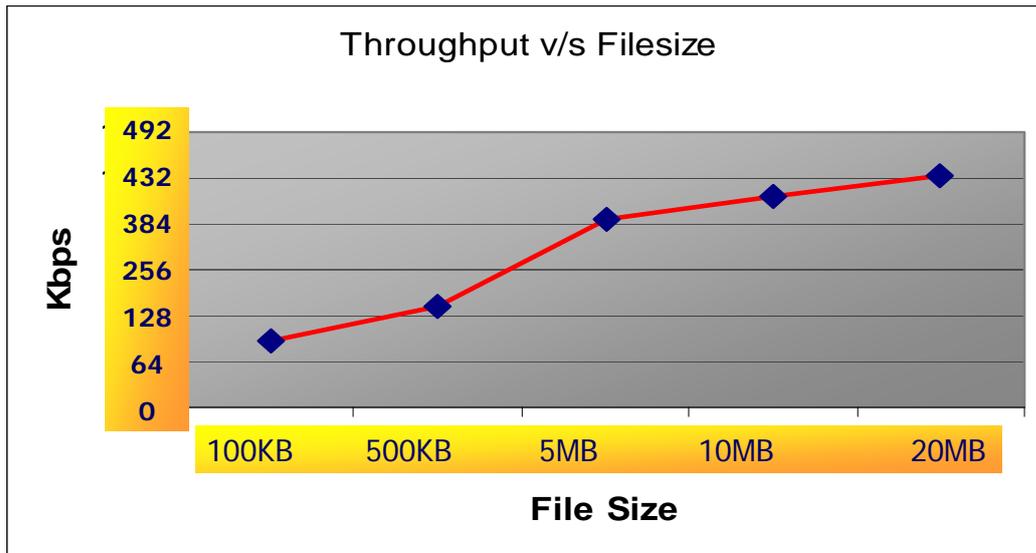


Figure 17 TCP Slow Start

6.5.2 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.

6.5.3 HTTP (Web Browsing) Slow Start

Web browsing can be affected by a combination of slow start and the FleetBroadband 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.

6.6 TCP Accelerator (TCP PEP)

6.6.1 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 FleetBroadband 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 FleetBroadband network
- Negating TCP slow start behaviour, further deteriorated by the round trip time between the terminal, satellite and ground segment.

6.6.2 TCP Accelerator Solutions

There are three types of TCP Accelerator solutions available from Inmarsat for use over the FleetBroadband 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 FleetBroadband 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 FleetBroadband 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.

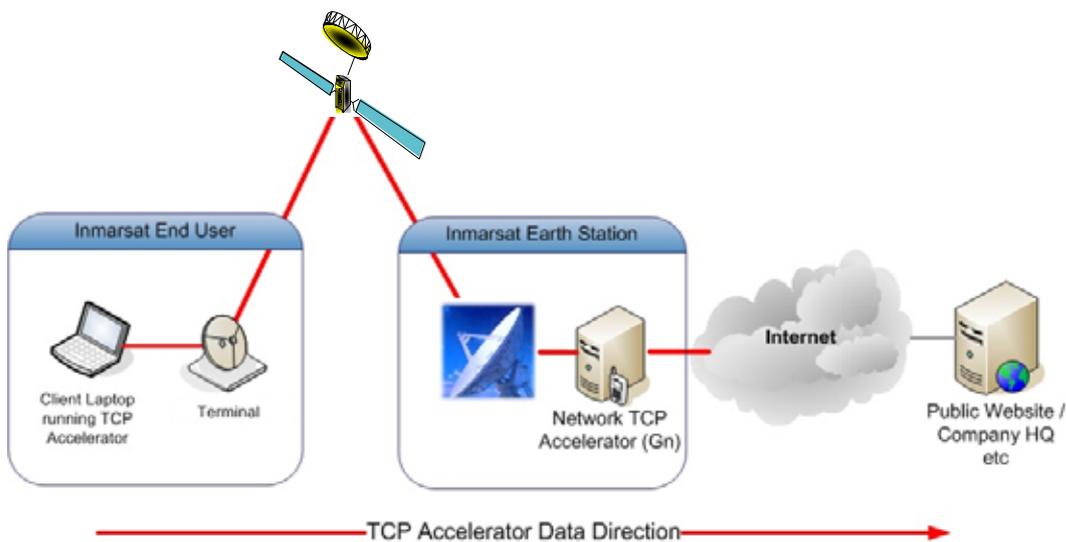


Figure 18 TCP Accelerator for FleetBroadband

The client application can be downloaded and installed on Windows and MAC operating systems from: <http://www.inmarsat.com/support>, click on **FleetBroadband**, then click on **TCP Accelerator**.

7. Connecting Peripheral Devices to the FleetBroadband Terminal

7.1 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 FleetBroadband 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 FleetBroadband 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.

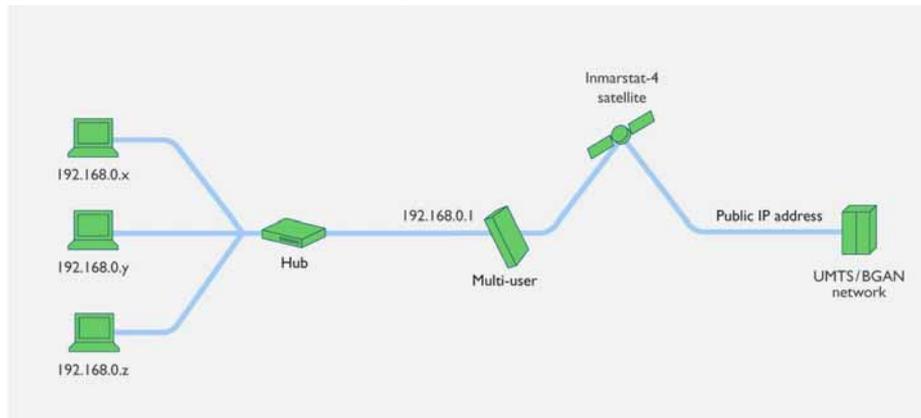
7.2 Network Address Translation (NAT) Mode

In NAT mode, the DHCP server in the terminal dynamically allocates IP addresses to 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 FleetBroadband 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.



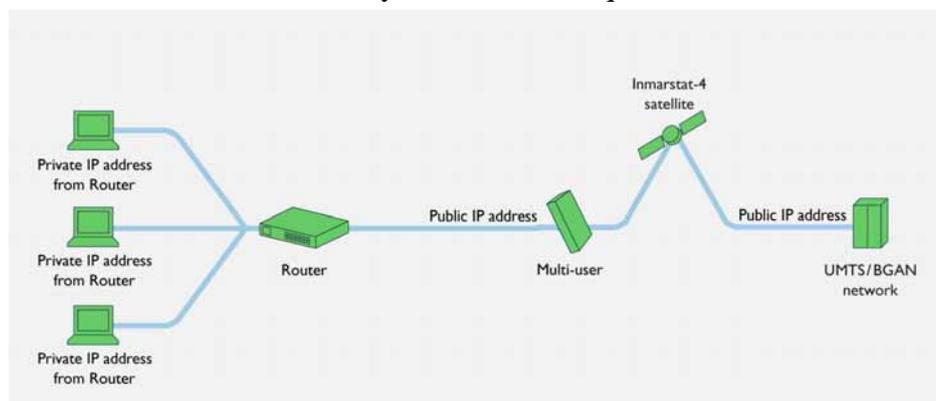
7.3 Modem Mode

In Modem mode, the terminal does not allocate IP addresses to the connected devices.

A single public IP address is allocated by your FleetBroadband Service Provider to the device connected to the FleetBroadband 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.



7.4 Port Forwarding

Port forwarding is carried out so that an external user can connect to a server that is 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.

7.5 IP Connections Explained

7.5.1 About PDP contexts

The FleetBroadband 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 FleetBroadband terminal and FleetBroadband 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 FleetBroadband core network. This request includes key information about the FleetBroadband terminal, for example:

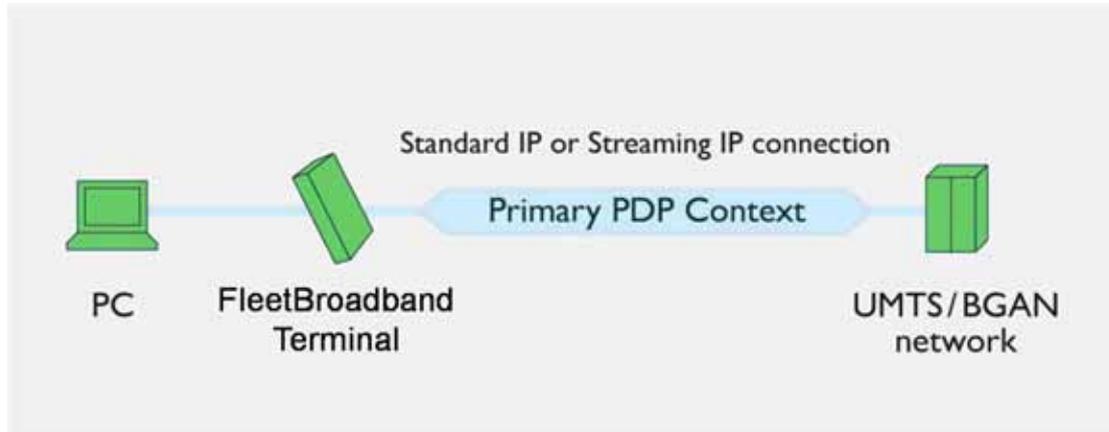
- the PDP address (which may be, for example, an IP address).
- the PDP type (that is, static or dynamic address).
- the QoS requested for this context – standard or streaming at the selected data rate.
- the Access Point Name (APN) of the external network to which connectivity is requested.
- your SIM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

On receiving the Activate PDP Context message, the FleetBroadband 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 FleetBroadband core network and data transfer can then take place between the terminal and the external data network.

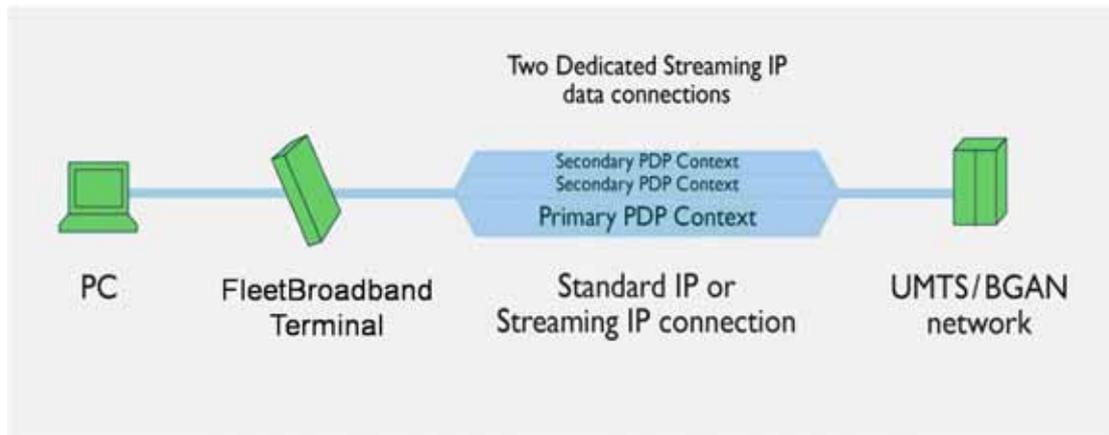
7.5.2 FleetBroadband and PDP contexts

The FleetBroadband terminal creates a PDP context for each IP data connection that you open to send or receive traffic over the FleetBroadband 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 FleetBroadband, the FleetBroadband 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 FleetBroadband 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.

7.5.3 About FleetBroadband Network IP addressing

When your FleetBroadband terminal connects to the FleetBroadband network it is assigned a IP address by your FleetBroadband 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 FleetBroadband in the following situations:

- when running web-servers, mail-servers, or FTP servers behind the FleetBroadband 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

7.5.4 How static IP addressing is provisioned

Your Distribution Partner 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 FleetBroadband - 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.

8. Maintenance, Support and Security Procedures

8.1 Training and Handover

The integration of FleetBroadband 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 FleetBroadband-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.

8.2 Remote Support

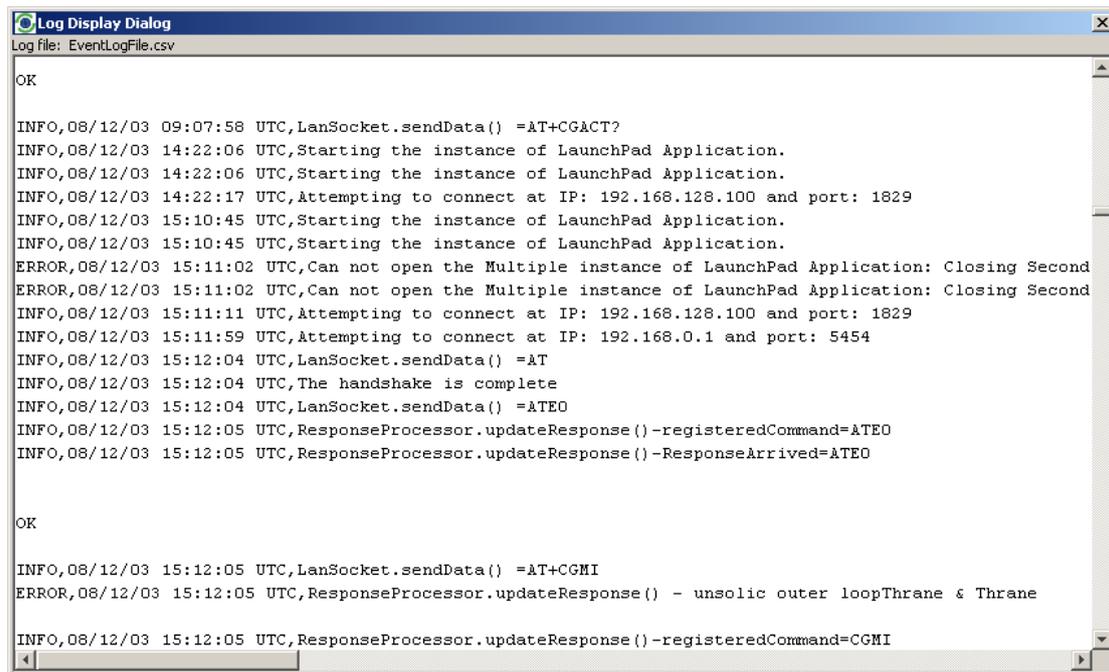
The ability to provide shore-based support for vessel-based networks and computers is one of the most important drivers for the implementation of FleetBroadband on ships. This benefit is further enhanced by the ability to run concurrent voice and data sessions on FleetBroadband so that voice communication 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).

8.3 Error Logging

The FleetBroadband 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.



```

Log file: EventLogFile.csv

OK

INFO,08/12/03 09:07:58 UTC,LanSocket.sendData() =AT+CGACT?
INFO,08/12/03 14:22:06 UTC,Starting the instance of LaunchPad Application.
INFO,08/12/03 14:22:06 UTC,Starting the instance of LaunchPad Application.
INFO,08/12/03 14:22:17 UTC,Attempting to connect at IP: 192.168.128.100 and port: 1829
INFO,08/12/03 15:10:45 UTC,Starting the instance of LaunchPad Application.
INFO,08/12/03 15:10:45 UTC,Starting the instance of LaunchPad Application.
ERROR,08/12/03 15:11:02 UTC,Can not open the Multiple instance of LaunchPad Application: Closing Second
ERROR,08/12/03 15:11:02 UTC,Can not open the Multiple instance of LaunchPad Application: Closing Second
INFO,08/12/03 15:11:11 UTC,Attempting to connect at IP: 192.168.128.100 and port: 1829
INFO,08/12/03 15:11:59 UTC,Attempting to connect at IP: 192.168.0.1 and port: 5454
INFO,08/12/03 15:12:04 UTC,LanSocket.sendData() =AT
INFO,08/12/03 15:12:04 UTC,The handshake is complete
INFO,08/12/03 15:12:04 UTC,LanSocket.sendData() =ATEO
INFO,08/12/03 15:12:05 UTC,ResponseProcessor.updateResponse() -registeredCommand=ATEO
INFO,08/12/03 15:12:05 UTC,ResponseProcessor.updateResponse() -ResponseArrived=ATEO

OK

INFO,08/12/03 15:12:05 UTC,LanSocket.sendData() =AT+CGMI
ERROR,08/12/03 15:12:05 UTC,ResponseProcessor.updateResponse() - unsolic outer loopThrane & Thrane

INFO,08/12/03 15:12:05 UTC,ResponseProcessor.updateResponse() -registeredCommand=CGMI

```

Figure 19 FleetBroadband Log Display

8.4 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

8.5 Standby PC and Ghost Images

Section 8.2 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.

8.6 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.

8.7 Access control

8.7.1 User levels

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

8.7.2 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.

8.7.3 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.

8.7.4 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>).

8.8 Scheduling

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

8.9 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 Distribution Partner 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.

9. Communication Cost Management

9.1 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 20 or is it intermittent like, for example, web-browsing as shown below in Figure 21?

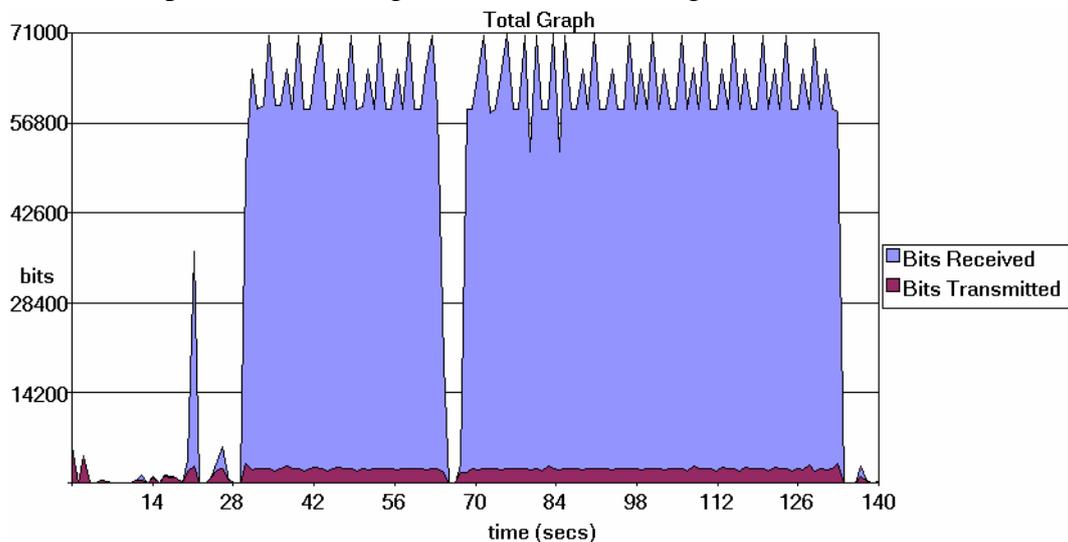


Figure 20 FTP Traffic Flow Profile

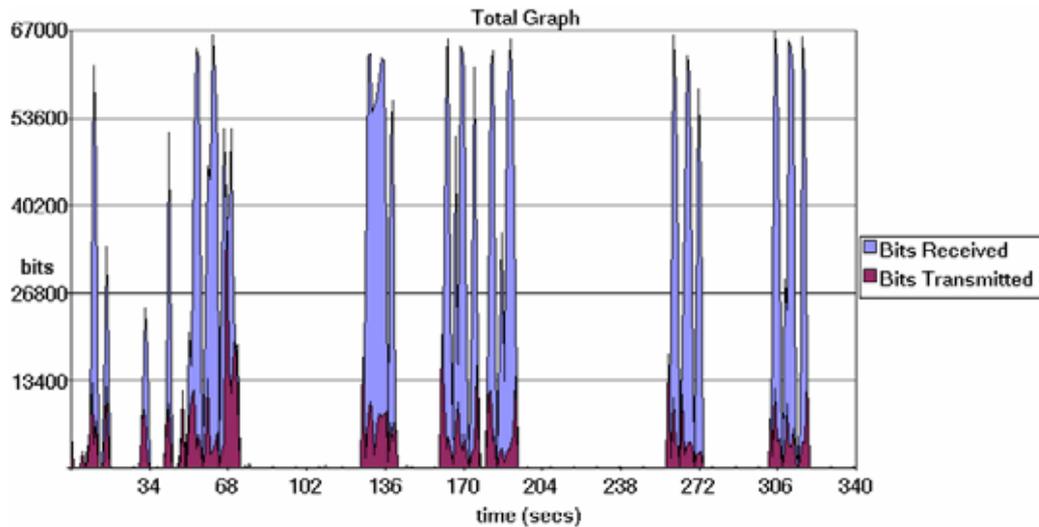


Figure 21 Web-browsing Traffic Flow Profile

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.

9.2 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
- Dialog
- Livewire – Selector Switch
- Virtek
- SeaWave - Integrator 3.0

9.3 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

9.3.1 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 Distribution Partner

9.3.2 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.

9.4 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 FleetBroadband 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:

1. 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.
2. 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.

9.5 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

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

9.6 Using Web-caching

Web-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.

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 FleetBroadband network connect to all sites that you are likely to use over FleetBroadband. This will **preload** your cache with the images etc from these sites.

9.7 Reducing Unnecessary LAN Traffic

9.7.1 Block unwanted traffic

When a client computer is connected to a FleetBroadband terminal with a network cable, the computer considers itself part of a LAN. The FleetBroadband 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.

9.7.2 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 FleetBroadband 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.

10. Applications Optimisation

10.1 Voice/VoIP

All of the FleetBroadband 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 FleetBroadband direct dial voice service is used in preference to IP-based telephony solutions.

10.2 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 FleetBroadband 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_sntp.asp
- E-fax http://home.efax.com/s/r/uk_home?CMP=OTC-uk
- On-Go <http://www.on-go.com/insol.html>

10.3 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 FleetBroadband 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.

10.4 Email

10.4.1 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.

10.4.2 Optimising email clients

Some Distribution Partners 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 if the recipient has a utility to uncompress the attachments.

Contact your DP for further advice in this regard.

10.4.3 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.

10.4.4 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.

10.4.5 Optimising Mozilla Thunderbird

The Thunderbird client is an open source equivalent to Outlook Express. Exactly the same modifications can be carried out to ensure that this client works optimally over FleetBroadband.

- 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.

10.4.6 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 Distribution Partners 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.

10.4.7 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.

10.5 Web browsing

10.5.1 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 Distribution Partner 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.

10.5.2 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

10.5.3 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 FleetBroadband 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.

The developers of the Opera browser claim that it is the fastest browser available and 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.

11. Operating System Optimisation

11.1 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 FleetBroadband 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).

11.2 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 FleetBroadband 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 FleetBroadband 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).

11.3 Mac OS Optimisations

Mac OSX is UNIX based, so knowledge of UNIX or Linux systems can help when optimising MAC for use over FleetBroadband.

The default TCP parameters for Mac OSX operate successfully over the FleetBroadband 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**.

12. How can you benefit from FleetBroadband?

12.1 Maritime Industry Trends

Changes in industry trends affecting all of shipping are driving many of the developments and integration challenges:

- Retention of skilled crew/seafarers – increasingly a limited resource.
- Significant growth in fuel costs as a proportion of total ship operations.
- Increased computerisation onboard, onshore, suppliers, ports etc.
- Remote support and maintenance
- Need for control/management - tighter integration between vessel and shore-office systems
- Boom in Oil & Gas
- Trade with China, SE Asia
- Increased Regulations – GMDSS, Ship Security Alert, LRIT
- Piracy, Terrorism, Security
- Shipyard boom

So how can FleetBroadband help you to address these challenges?

12.2 Ship Management Functions & Responsibilities

FleetBroadband is the communications hub for your onboard management systems as shown below in Figure 22

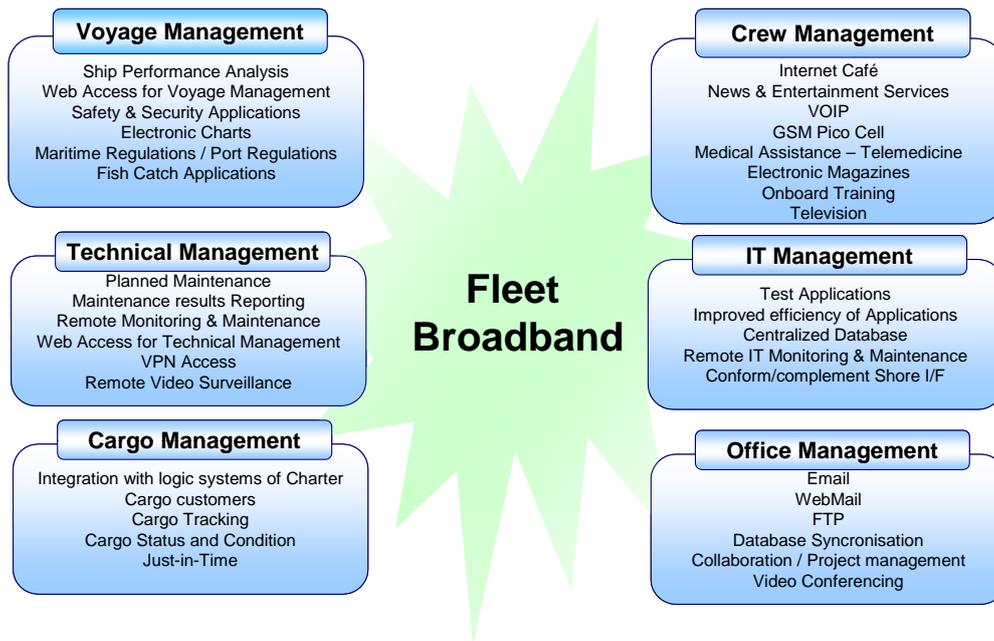


Figure 22 FleetBroadband Communications Hub

All of these management functions will generate or require data without which they cannot function. With the growing deployment of sophisticated IT networks and systems both onshore as well as onboard vessels, the power and flexibility of the FleetBroadband services will be invaluable:

- common front-end & user interface for all terminals.
- simultaneous voice, background-data and dedicated streaming-data
- SMS
- choice of data services and choice of charging options
- high data rates on both Standard IP and Streaming IP
- simple installation – reduced size, weight, downtime, cost
- wide range of applications can be deployed. No need for proprietary solutions (although some may be desirable)
- control and management benefits possible. e.g. training, maintenance.

12.3 Cost-Effective Ship Operations

The maximum benefit is achieved from FleetBroadband when it is used to implement solutions that actually optimise and reduce the overall cost of ship operations such as those shown in Figure 23 below, entitled Typical Ship Operating Costs.

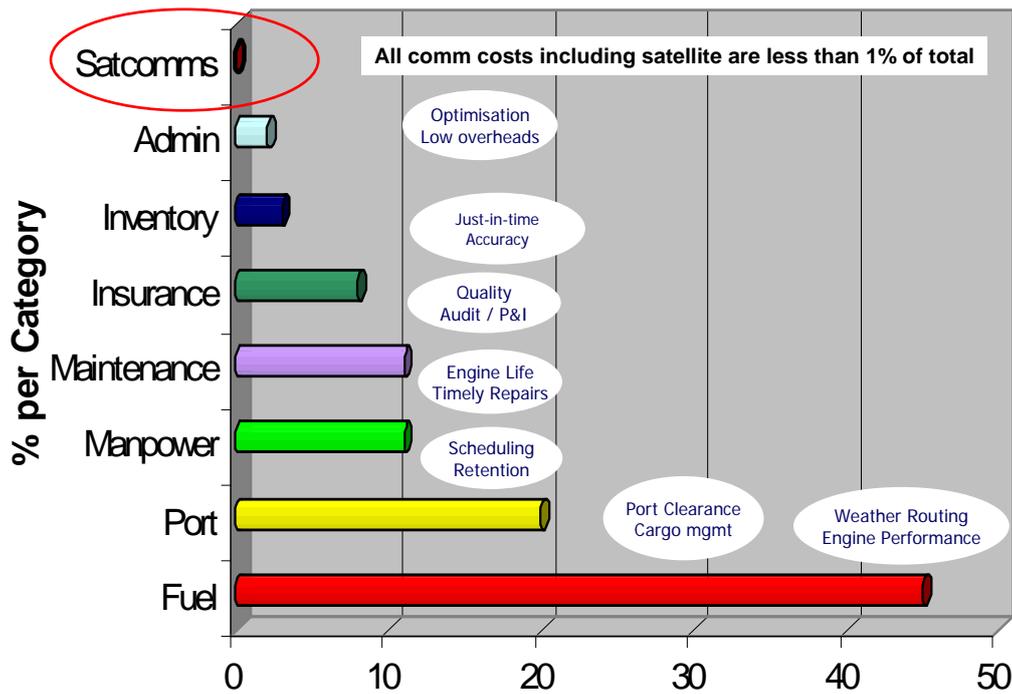


Figure 23 Typical Ship Operating Costs

Satellite communication charges are typically less than one percent of the total operating costs of a ship. If significant cost savings can be made in other areas of ship operations by the use of FleetBroadband then there will be a significant overall reduction in ship operating costs – even if the cost of the satellite communications actually increases.

12.4 Crew Welfare and Retention

A number of options are available. Our recommendations take into account various factors such as:

- Cost of implementation
- Complexity of deployment and management
- Availability of off-the-shelf solutions
- Nature of cost management and whether it will be sponsored by shipping company or paid for by crew themselves.
- The range of flexibility of access and freedom provided.

Some of the applications you may wish to consider are:

- Crew Calling (Voice and SMS)
- Crew Email and Internet

These are discussed in the following sections.

12.4.1 Crew Calling

Crew Pre-paid Calling Cards

Crew members are able to purchase pre-paid calling cards for use with the FleetBroadband terminal for their own personal use. Cards can be used for voice or SMS calls and are available from most Distribution Partners including:-

- Stratos - Stratos ChatCard www.stratosglobal.com
- Vizada – Universal Card www.vizada.com

GSM over FleetBroadband

GSM over FleetBroadband enables users to make and receive voice calls, send and receive SMS text messages using their own or pre-paid SIM cards in their personal mobile phones. The mobile phones on board the ship send and receive voice and data messages through the ship's own mobile base transceiver station. This base station is connected to the remote gateway which converts the data/voice signals received into a narrowband signal for transmission over the FleetBroadband network. GSM solutions for use over FleetBroadband can be obtained from several companies including:-

- Blue Ocean Wireless www.blueoceanwireless.com
- Zynetix www.zynetix.com
- Stratos GSM Oceanwide www.stratosglobal.com

12.4.2 Crew Email and Internet Access

Crew Email and Internet require most planning and should be deployed in a phased manner as suggested below:-

Phase 1

- Start from Email or Webmail – ideally using a specialist solution
- Implement only Chat-Cafe (MSN, Yahoo Messenger etc)
- Block everything else

Phase 2

- Implement fully-controlled PC's supplied by the ship
- Must use firewall, onboard caching and pre-compression
- Implement maximum control and restricted Internet access
- Preferably access Internet via corporate intranet

Phase 3

- Provide Wifi hotspots on vessel for crew PC access
- Implement appropriate caching/pre-compression middleware
- White-list/black-list management

Solutions that will assist you in implementing a successful crew calling programme include those from:-

- 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

12.5 Reduced fuel costs

Optimal routing and effective engine maintenance can help reduce fuel costs significantly through the implementation of state-of-the-art solutions.

12.5.1 Weather Routing

Weather information and chart plotting systems will benefit from the large bandwidth and lower costs per megabyte provided by FleetBroadband. This will enable vessels to receive data that is:-

- Higher resolution
- Greater coverage area
- Longer forecasts
- More frequent

Examples of such systems include those from:-

- ABS Nautical Systems www.abs-ns.com
- Jeppesen C-MAP www.c-map.no
- Transas Marine www.transas.com
- Chartco www.chartco.com
- Meteo Consult www.meteoconsult.fr

12.5.2 Engine Maintenance (Preventative and Predictive)

Engine maintenance solutions that will benefit from FleetBroadband include those from:-

- Front-line Communicator/Audisoft www.audisoft.net
- Sperry Marine www.sperrymarine.northropgrumman.com
- Wartsila www.wartsila.com
- MAN www.manbw.com

12.6 Imaging and Video Applications

12.6.1 Maritime Imaging and Video Applications

The bandwidth provided by FleetBroadband means that many imaging and video-based applications can now be made available for use by vessels. Some of the key maritime areas that could benefit from such applications include:

- Safety
- Training
- Remote Maintenance/Support/Control
- Security
- Insurance P & I
- Social/Crew Retention
- Legal
- Corporate

With the exception of video conferencing, which requires a Streaming IP link, all of these video and imaging applications can use the Standard IP data service.

12.6.2 Digital Photos

Transmission of high resolution photos for remote diagnostics, insurance assessment, medical assistance.

12.6.3 Video Chatting

MSN, Yahoo Messenger. Typified by webcam quality images during text-

conferencing sessions.

12.6.4 Store & Forward Video

High-quality high-resolution video files are captured on board, compressed and transferred to shore using FTP. Files captured and transmitted in this manner are usually very large but are of broadcast quality eg. Clipway Challenges.

12.6.5 Video Streaming

Typically text/audio/video transmitted in one direction. Systems are available from several suppliers including Frontline Communicator, Real Video, MS Media, Livewire, Quicktime, Streambox, Quicklink, Media Clipway.

12.6.6 Video conferencing

Typified by high quality audio/video transmission synchronised in both directions. Users expect high quality images and good audio clarity which require the use of a Streaming IP connection with a guaranteed QoS. Systems and components are available from suppliers such as Motion-Media, Livewire, Tandberg, Polycomm PVX, Motion Media, Axis/Sony PTZ cameras, Ulead/Picasa.

12.7 Ship Management Applications

Corporate enterprise solutions such as Oracle, SAP, CRM and ERP are becoming increasingly widespread.

If such a system is to be used in conjunction with the FleetBroadband 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

12.8 Fishing Applications

Numerous services are available to the fishing industry which enhance the efficiency of the fishing process throughout the value chain. Such services range from navigation, imaging and fish location through to market information and regulatory compliance. All of these services can be accessed using the FleetBroadband service.

12.8.1 Geoeye

www.geoeye.com

GeoEye provide the SeaStarSM Commercial Fishing Service. Using GeoEye's OrbView®-2 satellite, plankton concentration data is collected, combined with oceanographic and meteorological information and processed. From there it is sent directly to the fishing vessel where the captain can use it to navigate to the closest and potentially most plentiful fishing areas.

12.8.2 Catsat

www.catsat.com

Catsat uses ocean-observing satellites and marine meteorology to help fishermen to:

- locate favourable fishing grounds
- reduce operating costs
- improve safety during fishing operations
- meet their quotas more efficiently

12.8.3 PEFA

www.pefa.com

Pefa is Europe's largest marketplace for fresh fish. Using an Internet-based sales system, buyers can purchase fish directly from 12 member auctions in Sweden, Denmark, the Netherlands, Belgium and Italy. Fishermen can profit from an online multi-lingual database of market information and statistics on price and demand for different types of fish across Europe.

12.8.4 Maxsea

www.maxsea.com

MaxSea provides a package of AIS and ARPA target tracking, routing and performance modules, 2D/3D displays and bathymetrics for use by commercial fishermen.

12.8.5 Traceall

www.traceall.co.uk

Traceall provides tracking and monitoring solutions for high value products including fish which to enable a supplier to remotely monitor and protect the integrity of their supply chain by delivering continual real time visibility of the environment.

12.8.6 Tracefish

www.tracefish.org

TraceFish was the short title for the "Traceability of Fish Products" concerted action project which ran from 2000-2002, co-ordinated by the Norwegian Institute of Fisheries and Aquaculture (Fiskeriforskning).

The main outcome of TraceFish was three consensus-based standards for recording and exchange of traceability information in the seafood chains.

These standards now form the basis for numerous traceability implementations in the industry, both privately funded projects and pilot R&D projects with public funding.