Thuraya IP Voyager

User Guide

Revision 4
3500883-0001

PROPRIETARY NOTICE

All rights reserved. This publication and its contents are proprietary to Hughes Network Systems, LLC. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Network Systems, LLC, 11717 Exploration Lane, Germantown, Maryland 20876.

HUGHES, HughesNet, IPoS, SPACEWAY, AIReach, Broadband Unbound, and Connect to the future are trademarks of Hughes Network Systems, LLC. All other trademarks are the property of their respective owners.

Copyright © 2014 Hughes Network Systems, LLC

Safety Information

For your safety and protection, read this entire user guide before you attempt to use the Thuraya IP Voyager. In particular, read this safety section carefully. Keep this safety information where you can refer to if necessary.

Warning Symbols Used in this Guide

This section introduces the various types of warnings used in this document to alert you to possible safety hazards.



WARNING

Potential radio frequency (RF) hazard. Where you see this alert symbol and WARNING heading, strictly follow the warning instructions to avoid injury to eyes or other personal injury.



WARNING

Where you see this alert symbol and WARNING heading, strictly follow the warning instructions to avoid personal injury.



DANGER

Electric shock hazard: Where you see this alert symbol and DANGER heading, strictly follow the warning instructions to avoid electric shock injury or death.

WARNINGS FOR THE THURAYA IP VOYAGER TERMINAL



Do not stand at the side or top of the Antenna (ADU)

This device emits radio frequency energy when in the transmit mode. To avoid injury, do not place head or other body parts at the side or top of the ADU when system is operational. Maintain a distance of one meter away from those areas of the ADU.



Properly ground the Below Deck Unit (BDU)

Failure to properly ground the terminal BDU may result in severe personal injury or death. Use the GROUND terminal on the BDU and follow the instructions found in the Installation manual.



General

Handle your Thuraya IP Voyager with care. The ADU is weather resistant per IEC 60529 IP56; however, do not submerge the unit. Avoid exposing the Thuraya IP Voyager to extreme hot or cold temperatures outside the range -25ºC to +55ºC.

Avoid placing the terminal BDU close to cigarettes, open flames or any source of heat.

Changes or modifications to the terminal BDU not expressly approved by Hughes Network Systems could void your authority to operate this equipment.

Only use a soft damp cloth to clean the terminal BDU.

To avoid impaired performance, please ensure the unit's ADU is not damaged or covered with foreign material like paint or labelling.

When inserting the SIM, do not bend it or damage the contacts in any way. When connecting the interface cables, do not use excessive force.



In the vicinity of blasting work and in explosive environments

Never use the Thuraya IP Voyager where blasting work is in progress. Observe all restrictions and follow any regulations or rules. Areas with a potentially explosive environment are often, but not always, clearly marked. Do not use the Thuraya IP Voyager while at a petrol filling station. Do not use near fuel or chemicals.



Qualified service

Do not attempt to disassemble the ADU or terminal BDU. The unit does not contain consumer-serviceable components. Only qualified service personnel may install or repair equipment.



Accessories

Use Hughes approved accessories only. Use of non-approved accessories may result in loss of performance, damage to the IP Voyager, fire, electric shock or injury.



Connecting devices

Never connect incompatible devices to the Thuraya IP Voyager. When connecting the Thuraya IP Voyager to any other device, read the device's User Manual for detailed safety instructions.



Pacemakers

The various brands and models of cardiac pacemakers available exhibit a wide range of immunity levels to radio signals. Therefore, people who wear a cardiac pacemaker and who want to use the Thuraya IP Voyager should seek the advice of their cardiologist. If, as a pacemaker user, you are still concerned about interaction with the Thuraya IP Voyager, we suggest you follow these guidelines:

- Maintain a distance of 20cm from the Wi-Fi antenna and your pacemaker:
- Maintain a distance of one meter from the main ADU front and sides and your pacemaker;
- Refer to your pacemaker product literature for information on your particular device.

If you have any reason to suspect that interference is taking place, turn off your Thuraya IP Voyager immediately.



Hearing aids

Most new models of hearing aids are immune to radio frequency interference from satellite terminals that are more than 2 meters away. Many types of older hearing aids may be susceptible to interference, making it very difficult to use them near a terminal. Should interference be experienced, maintain additional separation between you and the IP Voyager.



Electrical Storms

Operation of the Thuraya IP Voyager during electrical storms may result in severe personal injury or death. Ensure the BDU Equipment is properly grounded to the vehicle chassis.

INFORMATION TO USER

Hughes Network Systems, LLC, declares under our sole responsibility that the product Hughes 9105 Satellite IP Terminal to which this declaration relates, is in conformity with the following standards and/or other normative documents: ETSI EN 301 444, ETSI EN 300 328, ETSI EN 301 489-1, ETSI EN 301 489-17, ETSI EN 301 489-20, IEC 60950-1. We hereby declare that all essential radio test suites have been carried out and that the above named product is in conformity to all the essential requirements of R&TTE Directive 1999/5/EC and RoHS-2 Directive 2011/65/EU.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures.

- Reorient or relocate the receiving ADU
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contents

SAFETY INFORMATION ..... **I**

WARNING SYMBOLS USED IN THIS GUIDE I
WARNINGS FOR THE THURAYA IP VOYAGER TERMINAL II

CONTENTS ..... **V**

INTRODUCTION **1**

FIRST TIME SET-UP **1**

QUICK REFERENCE **2**

GLOBAL POSITIONING SYSTEM OPERATION 2
INTEGRATED STATUS DISPLAY 2
WEB MAN MACHINE INTERFACE (WMMI) SCREENS 3
HOME SCREEN *4*
PROPERTIES SCREEN *5*
STATISTICS SCREEN *6*
CONNECTION MANAGEMENT SCREEN *7*
STATUS SCREEN *8*
SETTINGS SCREENS *9*
NETWORK SETTINGS SCREEN *9*
PORT FORWARDING CONFIGURATION SCREEN *11*
SECURITY MANAGEMENT SCREEN *12*
ETHERNET MAC FILTERING CONFIGURATION SCREEN: *13*
LOGIN SETTINGS SCREEN *14*
WLAN CONFIGURATION SCREEN *15*
WLAN SECURITY SCREEN *16*
REMOTE ACCESS SCREEN *17*
ADVANCED SETTINGS SCREEN *19*
UPGRADING THE THURAYA IP VOYAGER 20
UPGRADING SOFTWARE *20*

TROUBLESHOOTING **22**

GENERAL TROUBLESHOOTING 22
STATUS CODES 25

GLOSSARY **37**

SPECIFICATION **39**

INDEX **41**

Introduction

Your Thuraya IP Voyager terminal provides mobile, high-speed data communications via satellite. Using "Always On" technology, you can remain connected to the Internet while only sending or receiving the data that you need at speeds of up to 444kbits/s, just as if you were sitting at your office desk.

The Thuraya IP Voyager works with your computer using an Ethernet or Wi-Fi connection much like commercially available wireless routers. Note that the Wi-Fi Access Point in the Thuraya IP Voyager uses a separate subnet and DHCP server than the wired Ethernet port. An internal router allows IP traffic to flow seamlessly between the two subnets and out over the satellite link.

While the Thuraya IP Voyager operates very similarly to other data modems that you may be familiar with, there are a few important operating differences to note. Please read this user guide carefully to understand all the aspects of operating your Thuraya IP Voyager.

First Time Set-Up

Please refer to the installation manual for the Thuraya IP Voyager terminal as it applies to your installation.



Do not stand in front of the Antenna (ADU)

The ADU emits radio frequency energy when in the transmit mode. To avoid injury, do not place head or other body parts at the side or top of the ADU when system is operational.

Quick Reference

This section serves as a reference guide, identifying the key operational aspects of using the Thuraya IP Voyager system and the **Controls and Indicators** on the Thuraya IP Voyager and their functions.

Global Positioning System Operation

The Thuraya IP Voyager contains an integrated Global Positioning System (GPS) receiver that is used to provide location information. GPS location information is required for system access, and the reception of a new GPS location is attempted automatically every time Thuraya IP Voyager is powered on. The GPS receiver is located in the antenna, otherwise known as the Above Deck Unit (ADU). It is updated automatically during operation provided the ADU is able to receive the GPS signal.

Integrated Status Display

The terminal BDU has an **Integrated Status Display** which allows you to view the operational status of the terminal. The display includes four lights for this purpose as explained in the following table



Light	Colour	Description
Power	Green	On when the BDU is powered up (light is embedded in the power switch)
Network Connection	Green	On when a network connection has been established (light is next to the world icon)
GPS	Green	On when a valid GPS location has been obtained (light is labelled GPS)
Fault	Red	On when the Thuraya IP Voyager has detected a fault, check the web user interface for additional information (light is next to the warning icon)

Web Man Machine Interface (wMMI) Screens

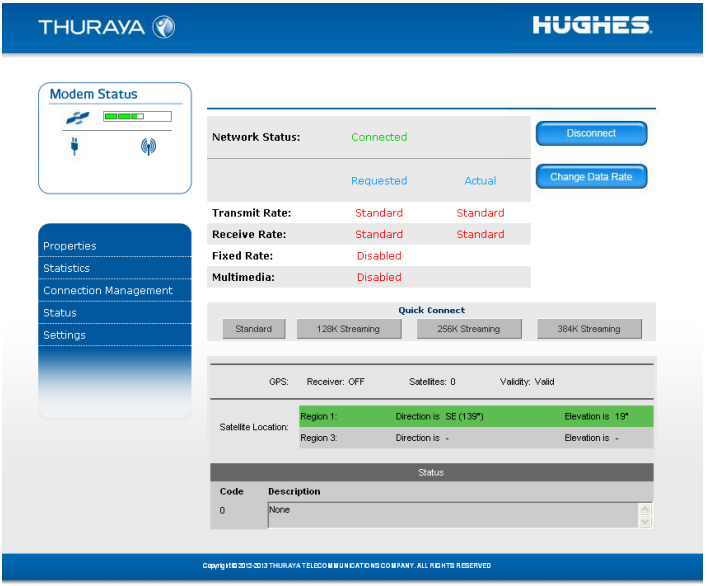
The Thuraya IP Voyager can be accessed through a standard web browser interface. To accomplish this, the connected computer must have one of the following supported browsers installed along with Java enabled (Java Runtime Environment 1.3.1 or later).

- Internet Explorer 6.0 or later
- Firefox 2.0
- AOL Explorer
- Macintosh Safari

To access the Thuraya IP Voyager, connect your computer via Ethernet or WLAN, run a supported browser and enter http://192.168.128.100 into the browser's address field. You may wish to add this address to the browser's bookmark list so the address will be easier to find in the future. When active, the browser interface will allow you to access the wMMI.

Each of the main web pages contains important status information in the upper left hand corner. The bar graph next to the  icon represents receive signal strength. During a streaming session this area also maintains a timer to record how long the session has lasted.

HOME SCREEN



The **Home Screen** provides you with key summary status information about the Thuraya IP Voyager and is also a gateway into Thuraya IP Voyager management.

Network Status: Provides the status of the network connection.

Transmit Rate: Provides the requested and actual transmit channel data rate. The actual allocated data rate may vary from the one requested due to subscription or system capacity restrictions.

Receive Rate: Provides the requested and actual receive channel data rate. The actual allocated data rate may vary from the one requested due to subscription or system capacity restrictions.

Fixed Rate: Provides the status of the Fixed Rate control. Enable Fixed Rate when using a streaming connection that must match the requested data rate. If the rate is unavailable, the connection is denied.

Multimedia: Provides the status of the Multimedia control. Enable Multimedia when using streaming applications like Voice over Internet Protocol (VoIP) or live video playback.

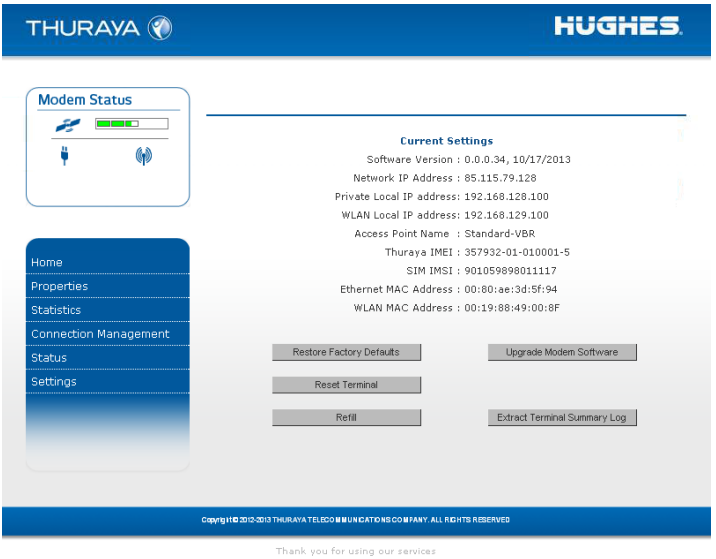
Connect/Disconnect: This button toggles the network connection state on or off. When disconnected no data can be sent or received.

Change Data Rate: This button allows you to change the connection parameters for the current session.

Quick Connect: These buttons access pre-stored connection profiles.

GPS: The display includes the GPS receiver state (On/Off), GPS satellites visible, GPS validity, compass direction and ADU angle. Once a GPS position is obtained, the Thuraya IP Voyager will provide the compass direction and degrees of elevation to the satellite. This information can be used to ensure that the ADU has a clear view of the Thuraya satellite at the current location.

PROPERTIES SCREEN



The **Properties Screen** displays a summary of current communications parameter settings. You can also use this screen to do the following:

Restore Factory Defaults: When you click this button, the **restore message confirmation screen** informs you that the terminal is about to reset to factory defaults. Restoring the factory defaults returns the Thuraya IP Voyager settings to their original, just out-of-the-box state. This does not change the security code or SIM parameters. Please exercise caution when proceeding. If you invoke **Restore Factory Defaults,** you will need to re-enter any configuration information supplied by your Service Provider.

Reset Terminal: Reboots the terminal software.

Refill: Connects to the prepaid SIM web site.

Upgrade Modem Software: Connects to the Thuraya upgrader web site.

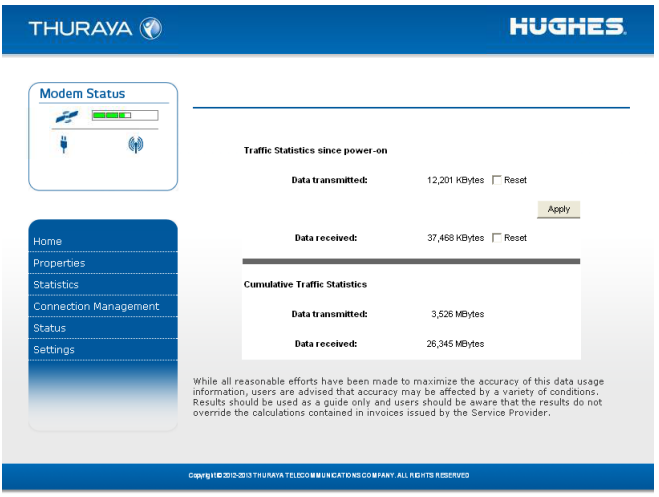
Extract Terminal Summary Log: Fetches diagnostic data from the terminal which can be saved on the connected computer.

Current Settings: provides the current communications parameters.

- Software Version currently installed
- Public Network IP Address
- Private Local IP Address (Ethernet subnet and wMMI address)
- WLAN Local IP Address (WLAN subnet)
- Access Point Name (APN) for the satellite connection
- BDU International Mobile Equipment Identity (IMEI)
- SIM International Mobile Subscriber Identity (IMSI)
- Ethernet and WLAN Media Access Control (MAC) Addresses

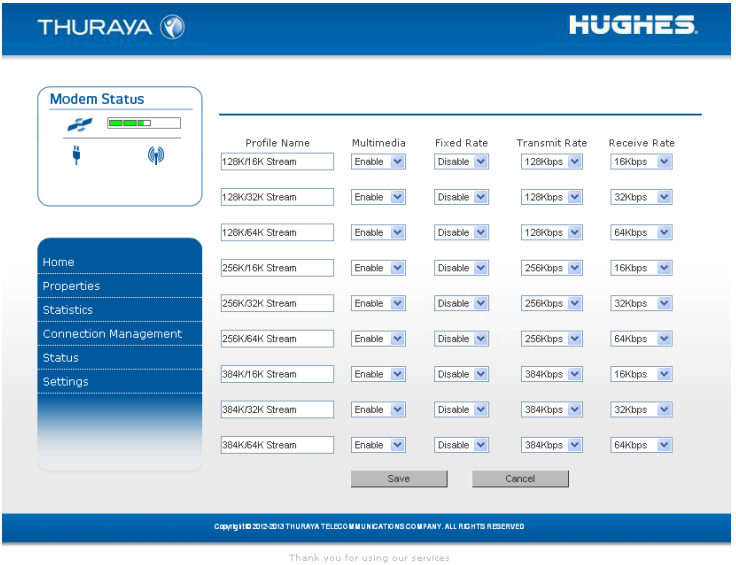
STATISTICS SCREEN

The **Statistics Screen** provides you with an estimate of your data usage. Data usage figures are obtained by counting the bytes in the IP packets received by and sent from the Thuraya IP Voyager. You can view both "since power on" (per session) and "cumulative" (lifetime) data usage counts. To reset the data counters of a session, simply select the **reset** button for either transmit or receive and click the **Apply** button.



Note: The data usage figures provided on the screen are estimates only. This feature is not tied into the actual billing system. Hughes assumes no liability if differences are found between data usage figures and your actual bill.

CONNECTION MANAGEMENT SCREEN



Accessible from the Main Menu, the **Connection Management Screen** allows you to select from nine Quality of Service (QoS) quick connect buttons. Each button can be customized using the **Details** link on the Connection Management Screen. The customization parameters for each button are as follows:

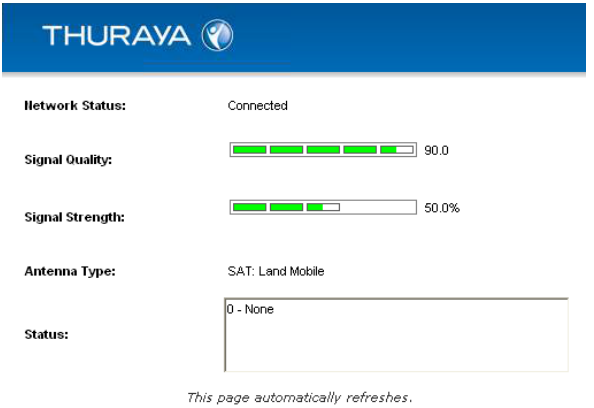
Transmit Rate and Receive Connection Rate: Allows you to select the transmit and receive rates from the list of bandwidth values.

Multimedia Control: Allows you to enable or disable Automatic Repeat-reQuest (ARQ) over the satellite. Typically, ARQ--an error control protocol for data transmission—is best disabled for voice or video traffic.

Fixed Rate Control: Allows you to enable or disable fixed rate service over the satellite. You can force the connection to match the requested QoS. If **disabled**, the best streaming rate possible -- up to and including the selected rate -- will be allowed. If **enabled**, the terminal will not set up a connection unless the requested rate is available from the network.

Remember to click **Apply** to save any changes or they will be lost.

STATUS SCREEN



The **Status Screen**, displayed in a separate window, provides you with a constantly updated flow of dynamic information and a concise summary of the Thuraya IP Voyager status.

When the **Status Screen** is open, its information is updated every minute.

Network Status: Provides the status of the network connection.

Signal Quality: This bar graph displays satellite signal quality.

Signal Strength: Use this display to monitor incoming signal strength from the satellite.

> **Note: Signal Quality vs. Signal Strength**. The Signal Quality status is a different measure of the received satellite signal than the Signal Strength status. Seeing differences between these two levels is normal and not an indication of a problem with your Thuraya IP Voyager unit.

ADU Type: Use this display to determine which antenna type is in use.

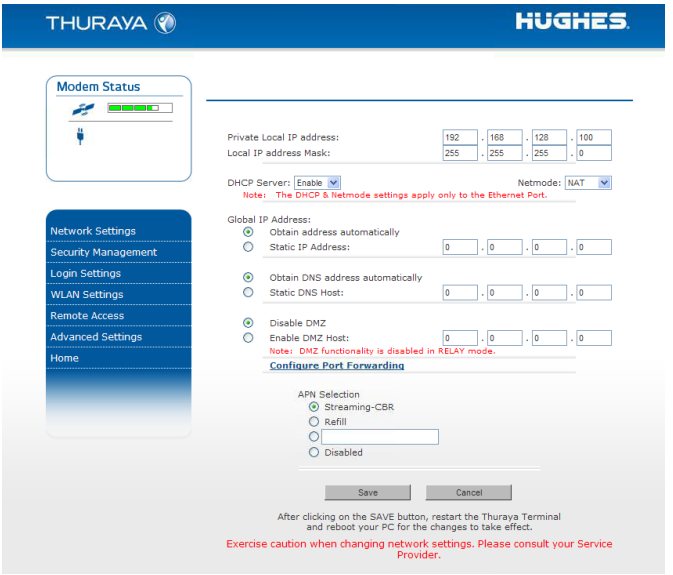
Status: Any current system status codes (see Troubleshooting section).

SETTINGS SCREENS

From the Main menu you can select **Settings** to navigate among all the various Settings functions from the menu on the left side of the screen:

- Network Settings
- Security Management Settings
- Login Settings
- WLAN Settings
- Remote Access
- Advanced Settings

NETWORK SETTINGS SCREEN



After executing the necessary First Time Set-up steps to configure the Thuraya IP Voyager, you may want to select the **Network Settings Screen** to check your network configuration. This screen provides you with control over key network access parameters. Here you find the appropriate Domain Name Service (DNS) and the Access Point Name (APN) information configured by your Service Provider. You are also given the ability to make changes.

> **Note**: Generally your Service Provider has already performed this configuration step for you. Whenever you modify the addresses on the Network Settings screen, you must press SAVE and exit the wMMI, reboot your computer, and power the Thuraya IP Voyager off and then back on so that the new settings can take effect.

Private Local IP Address: This setting allows you to change the all four octets of the terminal's (BDU) local gateway address. Changing this address will change the address of the wMMI and the base address for the Ethernet DHCP server. This subnet must remain unique from the WLAN subnet address being used.

Local IP Address Mask: This setting allows you to set the local Ethernet subnet mask. The setting for this mask should match the LAN that the terminal is connected to.

DHCP Server: The DHCP server for Ethernet can be enabled or disabled as needed. If disabled, a local static IP addressing scheme must be used by connected Ethernet devices. This setting has no impact on the WLAN operation which uses a dedicated DHCP server.

Netmode: This command allows for NAT or Relay Mode to be selected. The NAT (Network Address Translation) mode allows multiple devices to be connected via the Ethernet and WLAN ports. This is the default operating mode. Relay Mode is used for special situations where a single local device needs to be assigned the same address as the Global IP Address assigned to the terminal BDU. The connected device is assigned a LAN address initially, but with a very short DHCP lease time. When the Global IP Address is assigned to the terminal BDU it is flowed through to the connected device via a DHCP address reassignment. All WAN traffic flows through to the single connected device with no port or address translation. Relay Mode is only available on the Ethernet port and DHCP must be enabled at the same time on the connected device.

Global IP Address:

Obtain Address Automatically: If this button is **selected**, the Thuraya IP Voyager uses an IP address automatically assigned by the network during the period when the terminal connects to the network.

Static IP Address: If this button is **selected**, the Thuraya IP Voyager uses the IP address you enter in the associated IP Address field. You should check this box and enter an IP address only if directed to do so by your Service Provider.

DNS:

Obtain DNS Address Automatically: If this button is **selected**, the Thuraya IP Voyager uses a Primary Host Domain Name Service (DNS) automatically assigned by the network during the period when the terminal connects to the network.

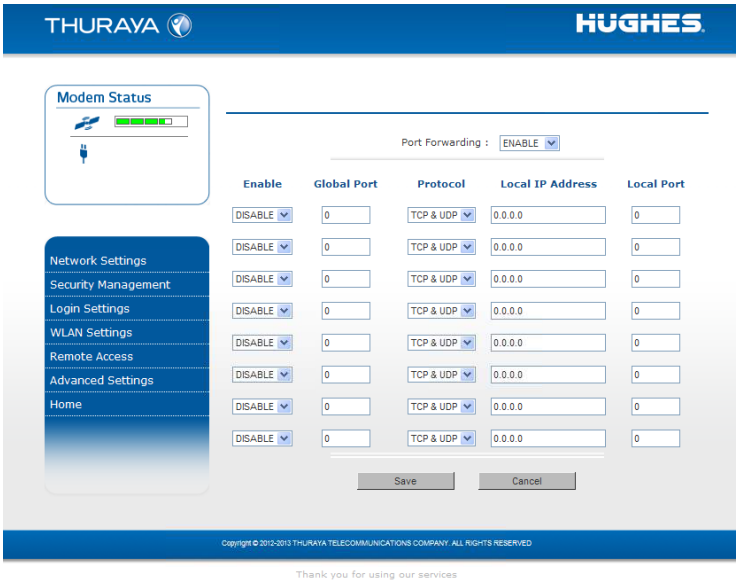
Static DNS Host: If this button is **selected**, the Thuraya IP Voyager uses the DNS address you enter in the DNS Address field. You should check this box and enter an IP address only if directed to do so by your Service Provider.

DMZ Host: If you wish to route incoming network originated IP traffic to a specific connected device, enter that device's IP address in this parameter. Be careful to establish a suitable firewall on this device to protect against malicious attacks from the Internet.

Port Forwarding: Port forwarding is a feature that allows user-specified global ports to be connected to user-specified TE devices. This mode allows incoming IP traffic to be reliably delivered to the specified TE IP address based upon the global port number the traffic was received on.

To enable/disable and to set up rules for port forwarding, click on the Configure Port Forwarding link to go to the Port Forwarding Configuration screen.

PORT FORWARDING CONFIGURATION SCREEN



Note that a new PDP context is required for Port Forwarding changes to take effect. Port Forwarding is not compatible with relay mode and is disabled automatically when relay mode is enabled.

APN Selection: If use of multiple Internet Service Providers is required, you can modify the current **Access Point Name (APN)** value. You should modify these fields only if directed to do so by your Service Provider. The choices are the following: Streaming-CBR, Refill, <BLANK> (enter the desired name) and Disabled.

SAVE/ CANCEL: If you want the values you have entered to be processed, click the **SAVE** button, **exit** the wMMI, and **reboot** your

computer. You will also need to turn the terminal BDU off and then on again so that the new settings can take effect. If you want the values you have entered to be ignored, click the **CANCEL** button and the Network Settings remain as they were with no reboot required.

SECURITY MANAGEMENT SCREEN



The **Security Management Screen** allows you to impose a tighter level of security on your Thuraya IP Voyager.

SIM PIN Disable/Enable: If **Enabled**, a prompt requests you to enter the SIM PIN each time you power up the modem. This helps prevent unauthorised use of your SIM. **Disable** this feature to skip the PIN entry process. To change the setting, click the desired one, enter the current SIM PIN (required), and click the **Save** button.

> **Note**: If the SIM PIN code is incorrectly entered three times, the SIM will be locked until the PUK (Pin Unlock Key) number is entered. Consult your Service Provider for the PUK number.

Change SIM PIN: If the SIM PIN is **enabled**, and you would like to change the existing PIN, click this link. You will be required to enter the Old PIN, the New PIN, and the New PIN again for confirmation.

Lock Upon SIM Change: When this setting is **enabled**, you must enter a security code when the terminal powers up with a new SIM.

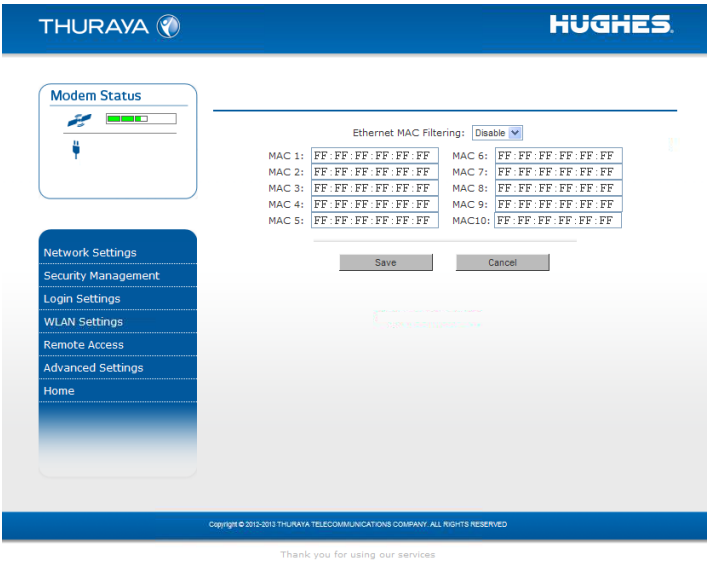
Restricted Administrative Access: When Restricted Administrative Access is **enabled**, protected web pages can only be accessed after you enter a username and password. The username is the fixed string "admin" and the password is the security code.

Change Security Code: The security code is 12345 when shipped from the factory. To change an existing Security Code, click this link. You will be required to enter the Old Code, the New Code, and the New Code again for confirmation.

> **Note**: If you forget the security code you will need to consult with your service provider.

Ethernet MAC Filtering: Ethernet MAC filtering provides a means to restrict Ethernet access to the UT to devices that have their MAC addresses specified in the white list. To enable Ethernet MAC filtering, click on the Ethernet MAC Filtering Configuration link on the Security Management Screen. This will take you to the Ethernet MAC Filtering Configuration Screen.

ETHERNET MAC FILTERING CONFIGURATION SCREEN:



From this screen you can enable and disable Ethernet MAC filtering and you can specify up to eight MAC addresses in the white list. Any changes to this configuration screen will be effective upon a restart of the UT.

Note: Enabling MAC filtering without specifying any entries in the list will disable the Ethernet ports in favour of WiFi access only. Be sure to enable WiFi on the UT before disabling the Ethernet ports so that you do not lose access to the wMMI.

LOGIN SETTINGS SCREEN

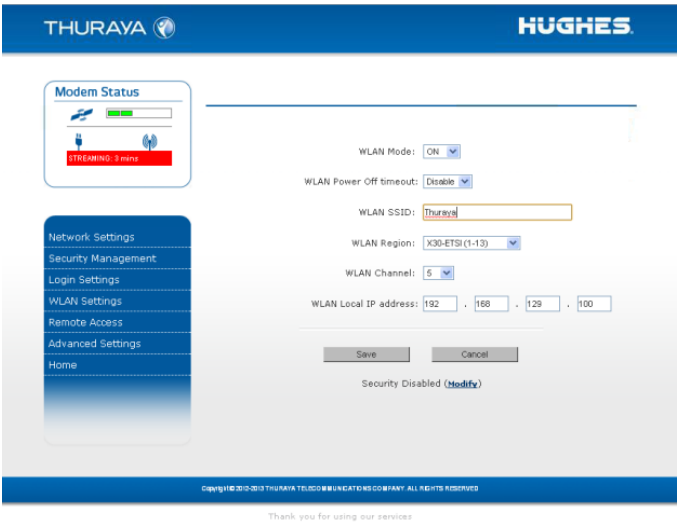


Utilize the **Login Screen** only if you have been given the necessary information from your Service Provider.

Service Provider Security: If this is **enabled**, you can enter a **User Name** and **Password** for authentication between the Thuraya IP Voyager and your Service Provider. Your Service Provider will let you know if this step is required and give you the necessary information.

User Name, Password, Confirm Password: You must enter the password twice to ensure accuracy.

WLAN CONFIGURATION SCREEN



The **WLAN Configuration Screen** allows you to configure the integrated WLAN Access Point (AP) which can support up to eight simultaneous clients using 802.11b/g/n. The WLAN AP operates on its own subnet and utilizes its own DHCP server. The wMMI remains at 192.168.128.100 (default) whether accessed via WLAN or Ethernet.

WLAN Power: Select ON or OFF to turn the feature on or off.

WLAN Power Off timeout: If **disabled**, there is no timeout. If this parameter is **enabled**, the WLAN will remain powered up for the selected timeout value after the terminal powers on. If no WLAN activity is detected during the timeout, the WLAN card will power down.

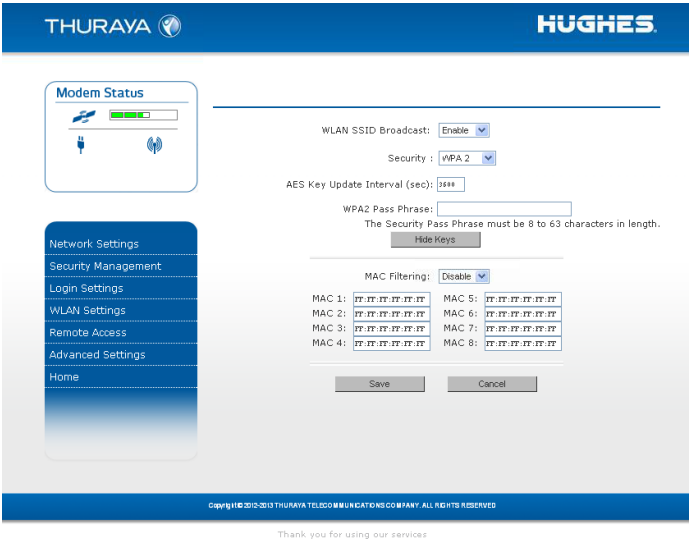
WLAN SSID: The WLAN network ID (SSID) can be entered as desired.

WLAN Region: Select the WLAN region from a drop down list (X10, X20, X30, X31, X32, X40 and X41). If you try to activate a channel not supported in the selected region, the request shall be rejected with an error message.

WLAN Channel: Select the WLAN channel from a drop down list.

WLAN Local IP Address: The WLAN network uses the default subnet of 192.168.129.xxx with DHCP addresses starting at 192.168.129.100. The two least significant octets can be changed to different values; however, the WLAN subnet must remain distinct from that used by Ethernet.

WLAN SECURITY SCREEN



The **WLAN Security Screen** allows you to configure WLAN security parameters, including enabling/disabling Wired Equivalent Privacy (WEP), hiding the SSID and setting Media Access Control (MAC) filters.

Access this screen by clicking the **WLAN Security Settings** link towards the bottom of the **WLAN Configuration Screen**.

WLAN SSID Broadcast: **Enable** or **Disable** SSID broadcast.

Security: **Disable** or chose an available security method: Wired Equivalent Privacy (WEP64 or WEP128), WPA or WPA2.

WEP Key to Use: Under WEP64, select the **active key**--Key1 through Key4--from a pull down menu. For WEP128 only key 1 is available.

WLAN Key Fields, Key 1 through Key 4: In WEP64 mode, enter a 10 character (0-9, A-F) **key value** in each of four text boxes. In 128-bit WEP mode, enter a 26 character (0-9, A-F) **key value** in the Key1 text box.

Generate: Instead of manually entering a key value, you may press the **Generate** button to automatically generate a key value.

TKIP/AES Key Update Interval: Under WPA and WPA2 this timeout determines how often the working key is changed.

WPA/WPA2 Pass Phrase: Under WPA and WPA2 enter a secret pass phrase as per the password policy length that will become the master key for WLAN access.

Hide Keys: Click this button to hide the keys from this display.

MAC Filtering: **Enable** or **disable** MAC filtering. If filtering is **enabled**, you can enter up to eight MAC addresses. Only these addresses will be permitted to access the terminal via the WLAN. MAC filtering changes only take effect after a power cycle of the terminal and are only enforced when some form of WiFi encryption is enabled.

REMOTE ACCESS SCREEN



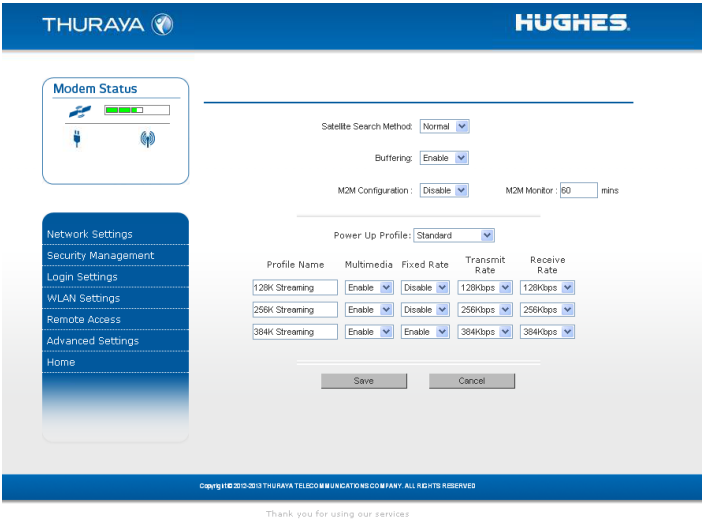
The **Remote Access Screen** enables wMMI access from the satellite side of the terminal. To use the feature, select the **Enabled** option, type in a password and select **Save**. Obtain the Network IP Address from the **Properties Screen** and use that in the browser on the remote PC as follows: http://85.115.79.53:45380 (85.115.79.53 is an example; your terminal address will be different and can change with each PDP session, depending on whether the network is issuing a dynamic IP address or static IP address). In general the IP address to use is http://aaa.bbb.ccc.ddd:45380, where aaa.bbb.ccc.ddd is your terminal's public IP address and the access port is 45380. You will need the remote access password to log into the terminal prior to gaining access to the wMMI. For security reasons you should use the **Logout** button on the wMMI once you have finished the session.

- Only one **Remote Access** session is supported at any one time
- The Thuraya IP Voyager must have an active PDP context in place
- The remote access password can be changed by entering a new string using the **Remote Access Screen** password entry

- The **Remote Access** feature is disabled by default
- If you forget the Remote Access password simply enter a new one to overwrite the old one.

Note that remote access does use satellite data that will be billed to the account on the user terminal. The remote access data also shares the channel with any other traffic being sent and received by the Thuraya IP Voyager.

ADVANCED SETTINGS SCREEN

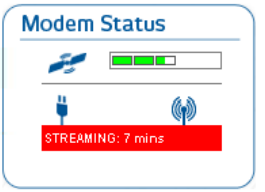


The **Advanced Settings Screen** allows you to modify several key operating parameters in the unit.

Satellite Search Method: **Normal** is the default method to use unless your Service Provider specifies the Full Method. The **Full** method takes longer and utilizes more resources since it will search all possible frequencies for the Thuraya IP service. This full search can take up to 20 minutes.

Buffering: When buffering is enabled the Thuraya IP Voyager can store more data to handle bursts of IP traffic from connected devices. When buffering is disabled, only the minimum of traffic is stored to reduce latency. Disable buffering for low latency traffic such as voice or video.

Streaming Alert: There is also a streaming timer embedded within the Modem Status box that appears on the upper left hand corner of the web page. This provides an indication of how long the streaming session has been active.



M2M Configuration: When enabled, the Thuraya IP Voyager will monitor the transmit and receive traffic. If traffic is not seen on either direction for the timeout duration then the terminal will automatically reboot to ensure it stays online. The feature will also try to re-establish a PDP context if it is disconnected for any reason. This mechanism is useful to ensure continuous operation from unattended installations.

M2M Monitor: This is the timeout setting for the M2M feature.

Power Up Profile: You can select the power up profile from a drop down list, including Standard and three customizable streaming profiles. Each streaming profile can be customized by **name**, **multimedia** mode, **fixed rate** mode, **transmit rate**, and **receive rate**.

Select the **Save** button to implement your modifications.

UPGRADING THE THURAYA IP VOYAGER

Should a Thuraya IP Voyager software upgrade become available, you can complete the upgrade process yourself. The software can be downloaded directly from the Internet using any available access method, including the Thuraya IP Voyager itself.

UPGRADING SOFTWARE

In order to upgrade software **you must first connect to the Internet** and follow the steps listed below:

1. Connect your PC/Notebook to the Internet using the Thuraya IP Voyager (satellite service), wired LAN, or dial up connection.
2. Go to www.thuraya.com or use the Upgrade link on the Properties Page if connected to the Thuraya IP Voyager.
3. Go to the web site area for Thuraya IP Voyager updates.
4. To download, select the latest upgrade package. The browser proceeds to retrieve the package.
5. Once the package is downloaded, you are prompted to execute the package. Select **Yes** and the upgrader application will self-extract onto the PC's hard drive.
6. Once the package is installed, it puts a shortcut on the desktop and prompts you to **upgrade now**. Make sure the Thuraya IP Voyager is now connected to the PC via Ethernet and is powered up. Select the upgrade option on the PC, and the program will allow you to upgrade the terminal BDU.
7. The upgrader will query the current software version of the terminal BDU. You should choose whether you want to upgrade to the newer version of software.
8. If you choose to upgrade the terminal BDU, the process automatically downloads the new release of software and forces a terminal reboot.
9. When the terminal BDU returns from reboot, you can verify that the download was successful via the ***Properties*** page in the wMMI or by confirming the new release on the upgrader.

10. Once loaded onto a PC, the upgrade program can be used to upgrade any number of Thuraya IP Voyager units. Just connect them one at a time and execute the upgrade program.

Troubleshooting

Some general hardware and software problems you may encounter in the installation and operation of Thuraya IP Voyager along with the possible source of these problems and how to correct them. System Status codes and descriptions reported to you by the Thuraya IP Voyager on the wMMI screens, along with their possible causes and solutions. If unable to correct a problem please contact the Thuraya IP Voyager dealer you purchased the unit from.

General Troubleshooting

Problem	Possible Cause	Action
Thuraya IP Voyager will not switch on.	DC input not present.	Ensure that between 10 to 32VDC is present at the terminal BDU power connector. Note extended DC cable runs may require a higher source voltage or lower resistance wire to ensure that the operating voltage is maintained under load.
	The remote switch line is not active.	The Thuraya IP Voyager will not power up unless the remote switch input has DC voltage applied.
	The fuse is blown or missing.	Check the blade fuse for connectivity and replace if necessary. Use only a 15 Amp, fast blow, ATO blade fuse, Littelfuse, part number 0287015.
	Insufficient current.	Ensure that the DC supply has sufficient current (12A) to supply the Thuraya IP Voyager.
SIM card error.	SIM card or SIM card contacts may be damaged.	Visually inspect the SIM card and SIM card contacts and return SIM card to your Service Provider if it is damaged.
	SIM card may not be present.	Verify that the SIM card is present.
	SIM card may be inserted incorrectly.	Remove the SIM card and make sure that it is inserted according to the instructions in the User Guide.

Problem	Possible Cause	Action
	SIM card contacts may be dirty.	Clean the SIM card contacts with a dry cloth.
The wMMI does not work from browser.	The browser may not be correctly configured.	For Firefox, go to Advanced Preferences and select 'Direct connection to the Internet.' For Microsoft Internet Explorer, select Tools / Internet Options / Connections / LAN Settings and uncheck the box labelled 'Use a proxy server for your LAN.' You May Need To Recheck This Box Upon Returning To Your Other Internet Connection.
Primary LAN connection to the BDU does not function.	The interface cable is not plugged in correctly.	Remove and reinsert the interface cable from both the PC and the BDU.
	The PC Windows network settings may not be configured correctly.	Make sure the Windows network settings in the PC are set to choose IP settings automatically (DHCP). Then reboot the PC.
	The PC can only have one active LAN connection. When connected to the PC, the terminal must be the only active LAN connection.	Disconnect all other LAN connections. Make sure the terminal is the only active LAN connection. Windows limits the number of network bindings to six. If you have more than six, you must remove one in order for the PC to communicate with the terminal.
The Security Code appears to be invalid.	The code may have been changed.	After ten failed attempts to enter the Security Code, you must switch the terminal off and on again to have access to another 10 retries. If you forgot the Security Code, contact your Service Provider.
The SIM PIN code appears to be invalid.	The code may have been changed.	If the SIM PIN is blocked, contact your Service Provider to obtain the PUK (PIN Unlock Key) code. Enter the PUK when prompted.
Thuraya IP Voyager cannot locate itself using	No signal or weak signal.	Make sure no obstruction is blocking the ADU. Make sure that you do not place any objects over the ADU.

Problem	Possible Cause	Action
GPS.	Determining GPS position can take up to 5 minutes.	Wait for 5 minutes. Switch the terminal off and on again.
	The ADU is not attached.	The ADU is required to be properly connected to the terminal BDU to obtain a GPS location.
Thuraya IP Voyager cannot find the satellite.	No signal or weak signal.	Make sure no obstruction is blocking the satellite signal. Make sure that the ADU has a clear view of the sky in the direction of the satellite.
Thuraya IP Voyager cannot access the internet.	PDP context disconnected.	Check the web MMI to ensure that a PDP connection has been requested.
	The ADU may be blocked.	You may need to reposition the Thuraya IP Voyager, verifying that there are no obstructions blocking the satellite signal and that the ADU has a clear view of the sky in the direction of the satellite.
	The terminal network settings may not be correctly configured.	Refer to the network settings supplied by your Service Provider. If the DNS Host settings are changed, the PC must be rebooted.
	The browser may not be correctly configured.	For Firefox, go to Advanced Preferences and select 'Direct connection to the Internet.' For Microsoft Internet Explorer, select Tools / Internet Options / Connections / LAN Settings and uncheck the box labelled 'Use a proxy server for your LAN.' YOU MAY NEED TO RECHECK THIS BOX UPON RETURNING TO YOUR OTHER INTERNET CONNECTION.
No network access or poor network performance.	Interference from other satellite mobile terminals.	If you are near another satellite mobile terminal, switch the other satellite mobile terminal off or move as far away as possible to avoid interference.

Problem	Possible Cause	Action
Thuraya IP Voyager stops sending data even with good network connection.	Terminal is overheated.	Let the Thuraya IP Voyager cool down before attempting to resume operation.
The Signal Quality meter on the wMMI changes from time to time.	Normal behaviour.	There are several types of channels used by the terminal, each with different signal strengths. Because the Signal Quality meter measures the channel currently in use, there may be slight differences in what the meter shows as channels are changed from one type to another.

Status Codes

Number and Description	Cause	Solution
1 SIM card is not installed. Power down, install SIM card properly and try again.	Absence or incorrect installation of the SIM card.	SIM card may not be present. Verify that the SIM card is present. SIM card may be inserted incorrectly. Remove SIM card and make sure it is inserted according to the instructions in the Installation Guide. SIM card may be damaged. Visually inspect the SIM card and return it to your Service Provider if damaged. SIM card contacts may be dirty. Clean the SIM card contacts with a dry cloth. If problem continues, replace SIM card with a known good SIM card. If problem persists, return the unit to your Service Provider for service.
2 SIM card read/write	Failure to read	Power down the Thuraya IP

Number and Description	Cause	Solution
error. Power down and try again.	from or write to the SIM card.	Voyager and try again. SIM card may be damaged. Visually inspect the SIM card and return it to your Service Provider if damaged. SIM card contacts may be dirty. Clean the SIM card contacts with a dry cloth. If the problem continues, replace SIM card with a known good SIM card. If the problem persists, return the unit to your Service Provider for service.
3 SIM card access has been blocked. Please contact your Service Provider.	Failure to access the SIM card due to too many failed attempts with an invalid PIN.	This occurs after 3 failed attempts to enter the PIN. The SIM card is locked. Enter the PUK to unlock the SIM card.
4 SIM card has been improperly changed during an active session. Power down and try again.	You replaced a SIM card with another after the terminal was turned on.	The SIM card must be replaced when the unit is turned off. Make sure the unit is turned off before replacing the SIM.
5 SIM card is not responding. Power down and try again.	Hardware failure to access the SIM card.	Power down the Thuraya IP Voyager and try again. SIM card may be damaged. Visually inspect the SIM card and return it to your Service Provider if damaged. SIM card contacts may be dirty. Clean the SIM card contacts with a dry cloth. If problem continues, replace SIM card with a known good SIM card. If problem persists, return the unit to your Service Provider for service.
6 A required data field is missing from the SIM card. Please contact	Absence of a required data field on the SIM	SIM card was incorrectly programmed and is missing one or more required fields. The SIM card

Number and Description	Cause	Solution
your Service Provider.	card.	must be replaced by another from your Service Provider.
7 You are not allowed to connect to the network. Please contact your Service Provider.	Network connection failure because the user is not allowed to connect to the Network.	Your authorisation has been removed by your Service Provider (SIM card IMSI is not authorised). Contact your Service Provider to regain service.
8 Your terminal is not allowed to connect to the network. Please contact your Service Provider.	Network connection failure because the terminal is not allowed to connect to the Network.	The terminal authorisation has been removed by your Service Provider (terminal BDU IMEI is not authorised). Contact your Service Provider to regain authorised service.
9 You have no subscription, service is not allowed. Ensure you are using a valid Thuraya SIM. Please contact SP if problem persists	Network connection failure because you are not identified as a subscriber to the service.	Contact your Service Provider to receive authorised service. Your Service Provider should check the subscription entries in the Home Location Registry.
10 The network detached the terminal, by the network. Verify your settings (APN, IP etc.) and retry.	Network connection broken with an unknown cause.	Verify settings, Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
11 Network connection failure - Invalid parameters used for network attach procedure. Please contact your Service Provider."	Network connection failure due to use of invalid parameters.	Contact your Service Provider.
12 Network connection failure - LLC or SNDCP failure. Power down and try again.	Network connection failure caused by LLC or SNDCP failure.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.

Number and Description	Cause	Solution
13 Network connection failure – Unknown PDP type. Please contact your Service Provider.	Network connection failure.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
14 Network connection failure - User authorisation failed. Please contact your Service Provider.	Network connection failure because the user is not authorised for service.	Contact your Service Provider to regain authorised service. Your Service Provider should check the subscription entries in the Home Location Registry.
15 Network connection failure – Service option not supported. Please contact your Service Provider.	Network connection failure because the service option is not supported.	Contact your Service Provider to regain authorised service. The Service Provider should check the subscription entries in the Home Location Registry.
16 Network connection failure - Service option not subscribed. Verify your settings (APN, IP, etc.) and retry. Please Contact SP if problem persists.	Network connection failure because user was not subscribed to the service option.	Verify settings and contact your Service Provider to regain authorised service. The Service Provider should check the subscription entries in the Home Location Registry.
17 Network connection failure - N-SAPI has already been used. Power down and try again.	Network connection failure because network assigned an N-SAPI that is already being used.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
18 Network connection failure – Regular PDP deactivation by network.	The connection was deactivated by the Network.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
19 Network connection failure - SM network failure. Power down and try again.	Connection failure due to the network Session Manager (SM).	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.

Number and Description	Cause	Solution
20 Network connection failure – Too many failures to activate PDP context. Power down and try again.	Too many failed attempts (4) to connect to the Network.	This failure may occur because of a weak signal due to obstructions or geographic position (such as extreme latitude or longitude). Contact your Service Provider to verify coverage for your location.
21 Network connection failure - Network assigned an invalid IP address. Power down and try again.	Assignment of an invalid IP address by the network during connection.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider. The Service Provider should verify that you have the correct network settings.
22 Network connection failure – No response from network. Power down and try again.	Network connection failure due to lack of a response from the network.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
23 Network connection failure – Protocol error received from network. Power down and try again.	Network connection failure due to a protocol error.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
24 Network connection failure – GPRS stack could not attach to MUX interface. Power down and try again.	Internal software error.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
25 Network connection failure - GPRS stack could not detach from MUX interface. Power down and try again.	Internal software error.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.

Number and Description	Cause	Solution
26 SIM card error - IMSI field is longer than 8 bytes and is invalid. Please contact your Service Provider.	SIM card may have been programmed incorrectly.	SIM card was incorrectly programmed. The SIM card must be replaced by another from your Service Provider.
27 GPRS software internal failure - GPRS stack message subscription failure. Please contact your Service Provider.	Internal software error.	Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
28 Your PC has been disconnected from the Thuraya IP Voyager. Please ensure the interface cable is plugged in securely.	The connection between PC and Mobile Terminal has been removed, or the interface cable between Terminal Equipment and Mobile Terminal is not plugged in properly.	Remove and reinsert the interface cable from both the PC and the Thuraya IP Voyager. When done reboot the Thuraya IP Voyager.
29 Your requested QoS parameters could not be met by the network. Please try again later	Current Network Resources cannot support the Quality of Service requested.	Try a different QOS setting.
30 Your requested QOS parameters are not valid. Please modify them and try again.	QOS selection incorrect	Check settings and If the problem continues, contact your Service Provider.
31 External ADU Comm Failure	ADU Fault: External Communication Failure between the ADU and terminal BDU.	Check ADU cable and restart terminal
32 ADU Cable Calib Failure	ADU Fault: Cable Calibration Failure between the ADU	Check ADU cable and restart terminal

Number and Description	Cause	Solution
	and terminal BDU	
41 Your PC is opening large numbers of TCP connections. The Thuraya IP Voyager is running out of resources.	Applications on your PC are generating excessive Internet connections.	Check your PC for applications that may open large numbers of connections and disable these applications. If the problem continues, contact your Service Provider.
42 TCP connection resources are depleted due to your PC opening excessive connections. You must restart your terminal to regain service to the network.	Excessive TCP connections by the PC have consumed all available connection resources in the terminal. The terminal cannot recover from this error.	Clean up PC applications that are consuming excessive TCP connections. Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
101 You were detached by the network. The Thuraya IP Voyager is attempting to reattach	Connection broken by the Network.	If terminal cannot reattach, Power down the Thuraya IP Voyager and try again. If the problem continues, contact your Service Provider.
102 No network connection, user initiated detach.	User initiated network disconnect.	User can reconnect using the wMMI connection controls.
103 Network connection failure – PLMN is not allowed. Reacquiring connection.	Network connection failure due to PLMN not allowed.	If the problem continues, contact your Service Provider.
104 Network connection failure - LA is not allowed. Reacquiring connection…	Network connection failure because the Thuraya IP Voyager is in a service not allowed Location Area (LA).	If the problem continues in other areas where service is allowed, contact your Service Provider.

Number and Description	Cause	Solution
105 Network connection failure – Roaming is not allowed. Reacquiring connection.	You are using a SIM card from a carrier that does not have a roaming agreement with your Service Provider.	If the problem continues with an authorised SIM card, contact your Service Provider.
106 Network connection failure – Thuraya IP Voyager implicitly detached by the network. Reacquiring connection…	Network connection failure because terminal was implicitly detached by the Network.	If the problem continues, contact your Service Provider.
107 Network service is not available – Network resources not available. Reacquiring connection…	Network service not available due to lack of network resources.	If the problem continues, contact your Service Provider.
108 Network service is not available. Reacquiring connection…	Network service not available.	If the problem continues, contact your Service Provider.
109 Network Service is not available - No Network. Move unit to a better coverage area and retry.	Network service not available.	If the problem continues, contact your Service Provider.
110 Access to the network is not available at the moment. Thuraya IP Voyager acquiring network. Power up the terminal under open sky and try again	Network service not available	If the problem continues, contact your Service Provider.

Number and Description	Cause	Solution
111 Network service is not available – Limited network service. Reacquiring connection…	Network service not available due to limited service.	If the problem continues, contact your Service Provider.
112 Network service is not available-Invalid position. Update the GPS under open sky and ensure you are under the Thuraya coverage.	Network service not available because the GPS position is not valid.	You should verify that the ADU has an open view of the sky to get a GPS fix. If the problem continues, contact your Service Provider.
113 Network service is not available – Invalid position for the selected Service Provider. Reacquiring connection…	Network connection failure because the of an invalid GPS position.	Verify that the ADU has an open view of the sky to get a GPS fix. If the problem continues, contact your Service Provider.
114 Network service is not available - Invalid position for selected RAI. Reacquiring connection…	The GPS fix does not match the selected Routing Area Information (RAI).	You should verify that the ADU has an open view of the sky to get a current GPS fix. If the problem continues, contact your Service Provider.
115 Network service is not available – Unknown cause. Reacquiring connection…	Network service not available – cause unknown.	If the problem continues, contact your Service Provider.
116 Network connection failure - Insufficient resources. Reacquiring connection…	Network connection failure due to insufficient resources.	If the problem continues, contact your Service Provider. Network may be down.

Number and Description	Cause	Solution
117 Network connection failure – PDP rejected for unspecified reason. Reacquiring connection…	Network connection failure – unknown cause.	If the problem continues, contact your Service Provider. Network may be down.
118 Network connection failure - Service option temporarily out of order. Reacquiring connection…	Network connection failure because service option is temporarily out of order.	If the problem continues, contact your Service Provider. Network may be down.
119 Network connection failure - PDP deactivated by network. Reacquiring connection…	Network connection failure.	If the problem continues, contact your Service Provider. Network may be down.
120 No network connection - User initiated PDP deactivation.	The terminal was powered down while connected to the network.	You will generally not see this code. In order for you to deactivate the PDP, you must power down the terminal. If the problem continues, contact your Service Provider.
121 Network connection failure - Missing or invalid APN. Please provide correct information and try again.	Network connection failure because the APN is missing or invalid.	Contact your Service Provider to get the correct network settings.
122 Network connection failure - Rejected by GGSN. Please re-enter User ID/Password and try again.	Network connection failure due to rejection by the GGSN.	Verify User ID/Password is correct on the network Settings Screen, re-enter and try again. If they are correct and the problem continues contact your SP.
123 Network connection failure - Subscribed QoS rejected by network. Please contact your	Network connection failure because the requested QoS was rejected	Modify the QoS settings and try again. If the problem continues, set all QoS settings to the default values and try again. If the problem continues with the

Number and Description	Cause	Solution
Service Provider.	by the Network.	default values, contact your Service Provider.
124 Network connection failure - Invalid transaction id. Reacquiring connection…	Network connection failure due to invalid transaction ID.	If the problem continues, contact your Service Provider.
125 Network connection failure – Unknown Session Manager error. Reacquiring connection…	Network connection failure due to unknown session manager error.	If the problem continues, contact your Service Provider.
126 Network access temporarily unavailable - Please wait, the Thuraya IP Voyager should automatically reacquire a connection within 1-2 minutes	Network connection failure because network access is blocked.	Network access is blocked. The network will send the terminal a timer value, and the terminal will attempt to connect again when the timer is complete. If the problem continues, contact your Service Provider.
127 Network access blocked - Radio priority is less than threshold. Thuraya IP Voyager waiting to be unblocked by the network.	Network access is blocked due to the user's priority.	You are blocked from Network access due to your network priority. If the problem continues, contact your Service Provider.
128 Network Blocked-GPS fix is too old. Please obtain new GPS fix in an open area away from obstructions. Please contact SP if problem persists.	Notification of a GPS fix during or after Network connection procedure.	A new GPS fix was obtained during the connection process, superseding the old fix. The terminal will reacquire the connection. If the problem continues and a new connection cannot be made, contact your Service Provider.
129 Network Access blocked-GPS location may be too old. Please	GPS fix may be too old.	Verify that the ADU has an open view of the sky to get a GPS fix. If the problem continues,

Number and Description	Cause	Solution
obtain new GPS fix in an open area away from obstructions. Contact SP if problem persists		contact your Service Provider.
130 Network access unavailable - GPS location needs updating. The Thuraya IP Voyager will acquire a new GPS location and connection. Do not power off!	GPS fix is too old.	The Thuraya IP Voyager will acquire a new GPS location and connection. Do not power off the terminal BDU.
132 Terminal temperature too high.	The terminal is too hot.	Allow the terminal to cool down.

Glossary

ADU: Above Deck Unit. The Thuraya IP Voyager tracking antenna.

APN: Access Point Name. APNs can be assigned to each external network interface to allow communications among multiple Internet Service Providers (ISPs). If use of multiple ISPs is required in your network, on Thuraya IP Voyager wMMI Network Settings screen you can enable APN and enter the value supplied by your Service Provider.

BDU: Below Deck Unit. The Thuraya IP Voyager inside vehicle unit.

DHCP: Dynamic Host Configuration Protocol. DHCP is a communications protocol that lets network administrators manage centrally and automate the assignment of IP addresses in an organization's network. With use of the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. You must make sure that the Windows network settings on your PC are set to allow the network to choose IP settings automatically.

DNS: Domain Name Service, a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses, allowing users of workstations configured to query the DNS to specify remote systems by host names rather than IP addresses. On Thuraya IP Voyager wMMI Network Settings screen, a primary and possibly a secondary DNS address supplied by your Service Provider must be assigned.

Ethernet: Ethernet is a local area networking method used widely throughout the computer industry.

GGSN: Gateway GPRS Support Node.

GPRS: General Packet Radio System.

GPS: Global Positioning System. When the GPS receiver in Thuraya IP Voyager gets a bearing on a GPS satellite, the receiver computes and stores the terminal's location on earth. That location is used in the Pointing Process to obtain your location relative to the Thuraya Satellite.

NAT: Network Address Translation.

Normal Operational Mode: In this mode, the Thuraya IP Voyager is connected to your network, allowing you to perform standard system activities such as Internet browsing.

PDP: Packet Data Protocol.

QoS: Quality of Service.

SIM: Subscriber Identification Module. Your Service Provider issues you a SIM, containing your SIM Personal Identification Number (PIN) and other security-related information. You insert the SIM into the terminal BDU SIM holder as part of terminal hardware setup. If you configure the terminal to enable SIM PIN security, each time you invoke the terminal wMMI after turning on the terminal, PIN authorisation is required in order to use the system.

SIM PIN: A Subscriber Identification Module (SIM) Personal Identification Number (PIN) may be supplied by your Service Provider. If SIM PIN entry is enabled on Thuraya IP Voyager wMMI Security Management screen, a prompt requests you to enter the SIM PIN each time you run the wMMI. This helps prevent unauthorised use of your SIM.

Static IP Address: A static Internet Protocol (IP) address is a number that is assigned to a computer by an Internet Service Provider (ISP) to be its permanent address on the Internet. Computers use IP addresses to locate and talk to each other on the Internet. If Static IP addressing is enabled on Thuraya IP Voyager wMMI Network Settings screen, you must enter an IP address supplied by your Service Provider in the Static Public Network IP Address field that follows.

Status Code: A number which uniquely references an event or condition in a hardware or software system. In Thuraya IP Voyager, if there is a fault detected, the status code and a description are displayed at the bottom of the terminal wMMI Home and Status screens.

Specification

Physical Characteristics	
Weight (BDU)	2.2 kg
Weight (ADU)	2.0 kg
Size (BDU)	46 mm x 281 mm x 233 mm
Size (ADU)	252mm x 119mm
Packet Data Services	
Streaming IP	384 kbps
Standard IP	444 kbps
Environmental	
Operating Temperature	-25°C to +55°C
Storage Temperature	-40°C to +80°C
Operating Humidity	95% RH at 40°C
Mechanical Vibration	200-2000 Hz, 0.3 m^2/s^3 MIL-Spec 810B
Unpacked Drop	0.5m (cosmetic damage only)
Ingress Protection (ADU)	IP56
Compliance and certifications	
	CE, EMC 301 444, 301 489, IEC 60950
External Power	
Main power input	10-32VDC
Maximum current	12A
Interfaces	
Connectors	4 Ethernet (PoE-IEEE 802.3af standard) Note: 48Vdc for PoE devices is supplied over the TX, RX pairs. It is active only when an 802.3af compliant device is plugged in. The other pairs (4, 5, 7, and 8) are unused.
User Interface	Web-based graphical user interface accessible via standard web browser
External Connector	Thuraya Satellite tracking antenna HN221(Land-mobile)
WLAN Connectivity	IEEE 802.11 b/g/n standard with: - WEP, WPA and WPA2 encryption - SSID broadcasting control - MAC address filtering - DHCP

Declaration of Conformity

Index

address 3, 10, 28, 36, 37
Administrative Access.....12
ADU.....2, 22, 23, 32, 34, 38
antenna.....ii, iv, 1, 5, 8, 22, 23
APN.....9, 11, 33, 36
ARQ 7
battery 24
BDU 1, 21, 23, 26, 36, 38
browser 2, 3, 19, 22, 23
compass 5
connection profiles.....5
data usage 6
DNS 9, 10, 23, 36
Ethernet 1, 19, 36
fault codes 21
Fixed Rate.....4, 7
GPS 2, 5, 22, 23, 32, 34, 35, 36
IMEI 6, 26
Java.....3
login.....13
MAC 6, 15, 16
Multimedia 4, 7
password 12, 13, 33
PIN.....11, 12, 22, 25, 37
pointing.....23
Power button 2
Private Satellite Modem IP Address 6
proxy server 22, 23
Public Network IP Address .. 6, 10, 37
QoS 7, 33, 37
Quality of Service 7, 37
region 14
Restore Factory Defaults 5
safety i
satellite .....ii, 1, 5, 7, 8, 19, 23, 36
security code 5, 12
Signal Quality 8, 24
Signal Strength.....8
SIM5, 11, 12, 21, 22, 24, 25, 26, 29, 31, 37
SSID..... 14, 15
temperature.....35
timeout.....14
upgrade..... 19, 20
USB.....1
video..... 4, 7
voice.....7
WEP 15
WiFi 1
WLAN 14, 15
wMMI ...3, 9, 11, 19, 21, 22, 24, 36, 37