Iridium® Short Burst Data Service Best Practice Guide

Release 2.0
November 27, 2017

Revision History

Version	Date	Reason
1.0	December 21, 2010	Internal Iridium Review
1.1	October 11, 2011	Internal Revision
2.0	October 8, 2017	Updated with optimal transmission intervals

Preliminary Product & Service Information Purpose & Disclaimer

Legal Notices:

This Iridium Short Burst Data Service Best Practice Guide provides administrative information and is provided "as is." Iridium and its affiliated companies, directors, officers, employees, agents, trustees or consultants ("Iridium") assume no responsibility for any typographical, technical, content or other inaccuracies in this Guide.

This document contains product and feature information for Iridium's Short Burst Data Service and Iridium Short Burst Data Only Transceivers. The purpose of providing this information is to enable Value Added Resellers and Value Added Manufacturers to better understand the best practices in using the Iridium SBD Service.

Iridium Communications reserves the right to modify or change information detailed herein at any time without notice, and does not make any commitment to update the information contained herein. See the Iridium SBD Developer's Guide for the Limited Warranty, Exclusions, Limitations and Conditions, as well as the Iridium Product Service Terms and Conditions, Warranty Support, Software License, and privacy-related information. Your use of the product as an Administrator is governed by the Iridium Product Sales Terms and Conditions which can be found at www.iridium.com

IRIDIUM MAKES NO REPRESENTATIONS, GUARANTEES, CONDITIONS OR WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED REPRESENTATIONS, GUARANTEES, CONDITIONS OR WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE OR TRADE PRACTICE, USE OR RELATED TO THE PERFORMANCE OR NONPERFORMANCE OF ANY PRODUCTS, ACCESSORIES, FACILITIES, SERVICES OR USER INFORMATION, EXCEPT AS EXPRESSLY STATED IN THE LIMITED WARRANTY AND THIS GUIDE. ANY OTHER STANDARDS OF PERFORMANCE, GUARANTEES, CONDITIONS AND WARRANTIES ARE HEREBY EXPRESSLY EXCLUDED AND DISCLAIMED TO THE FULLEST EXTENT PERMITTED BY LAW. THIS DISCLAIMER AND EXCLUSION SHALL APPLY EVEN IF THE EXPRESS LIMITED APPLICABLE TO THE SHORT BURST DATA SERVICE AND TRANSCEIVER (COLLECTIVELY THE "PRODUCT") FAILS OF ITS ESSENTIAL PURPOSE. NO WARRANTY IS MADE AS TO USER INFORMATION AND/OR COVERAGE, AVAILABILITY OR GRADE OF SERVICE PROVIDED BY IRIDIUM SEPARATELY FOR IRIDIUM SATELLITE SERVICES.

IN NO EVENT SHALL IRIDIUM BE LIABLE, WHETHER IN CONTRACT OR TORT OR ANY OTHER LEGAL THEORY, INCLUDING WITHOUT LIMITATION STRICT LIABILITY, GROSS NEGLIGENCE OR NEGLIGENCE, FOR ANY DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE COST OF THE IRIDIUM SATELLITE SERVICES PROVIDED. NOR SHALL IRIDIUM BE LIABLE FOR ANY ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF PRIVACY, LOSS OF USE, LOSS OF TIME OR INCONVENIENCE, LOSS OF INFORMATION OR DATA, SOFTWARE OR APPLICATIONS OR OTHER FINANCIAL LOSS CAUSED BY THE IRIDIUM SHORT BURST DATA SERVICE (INCLUDING HARDWARE,

SOFTWARE AND/OR FIRMWARE) AND/OR ACCESSORIES AND/OR THE IRIDIUM SATELLITE SERVICES, OR ARISING OUT OF OR IN CONNECTION WITH THE ABILITY OR INABILITY TO USE THE PRODUCT, ACCESSORIES AND/OR THE IRIDIUM SATELLITE SERVICES, TO THE FULLEST EXTENT THESE DAMAGES MAY BE DISCLAIMED BY LAW AND REGARDLESS OF WHETHER ADVISED OF THE POSSIBILITIES OF SUCH DAMAGES. IRIDIUM IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY.

Third Party Information

This Guide might refer to third party sources of information, hardware or software, products or services and/or third party web sites ("third party information"). Iridium does not control, and is not responsible for, any third party information, including without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of third party information. The inclusion of such third party information does not imply endorsement by Iridium of the third party information. ANY THIRD PARTY INFORMATION THAT IS PROVIDED WITH IRIDIUM'S FACILITIES, SERVICES, PRODUCTS OR USER INFORMATION IS PROVIDED "AS IS". IRIDIUM MAKES NO REPRESENTATIONS, GUARANTEES OR WARRANTIES IN RELATION TO THIRD PARTY INFORMATION AND IRIDIUM SHALL NOT BE LIABLE FOR ANY LOSSES, DAMAGES, LIABILITIES, JUDGMENTS, AND FINES, AMOUNTS PAID IN SETTLEMENT, EXPENSES OR COSTS OF DEFENSE SUSTAINED IN RELATION TO ANY SUCH THIRD PARTY INFORMATION.

Intellectual Property, Trade Secret, Proprietary or Copyrighted Information

To protect Iridium proprietary and confidential information and/or trade secrets, this Guide may describe some aspects of Iridium technology in generalized terms. Iridium products may include copyrighted Iridium and third party software. Any such copyrighted software contained in Iridium products may not be modified, reverse engineered, distributed or reproduced in any manner to the extent provided by law. The purchase of any Iridium products shall not be deemed to grant either directly or by implication or otherwise, any license under copyrights, patents, or patent applications of Iridium or any third party software provider. Except for the normal, nonexclusive, royalty free license to use that arises by operation of law in the sale of a product.

Content Copyright

You are exclusively responsible for your use of the Iridium Short Burst Data Service, including proper use of third party copyrighted materials. If you violate these terms, you agree to defend, indemnify and hold Iridium harmless with respect to any claims or actions by third parties related to your improper use of copyrighted material and to pay all costs, damages, fines and other amounts incurred by Iridium, or on its behalf, in the defense of any such claims or actions.

Table of Contents

1.0 Introduction

1.1 Purpose & Scope

This document is for Iridium's contracted Value-Added Resellers and Value-Added Manufacturers. It describes the best practices in using Iridium's Short Burst Data Service (SBD). This document is a supplement to the SBD Developer's guide and additional information about the SBD services is contained in this document.

Additional documentation is available from the Iridium for partners section of the www.iridium.com web site. This section of the website is available only to authorized Value Added Manufacturers or Value-Added Resellers.

2.0 SBD Operational Overview

The SBD service is a success based protocol, the response codes returned to the sender indicate if the message was successfully received by the next node or not. There are two types of message types that are delivered via SBD Services, Mobile Originated (MO) and Mobile Terminated (MT) messages.

2.1 Optimizing transmission intervals

This section highlights good practices that will ensure monitoring applications are best positioned for shortest latency and message delivery. Often, applications or software try and transmit data right after it was sampled, even though the criticality of delivery is not that high. Well-designed applications often use "measurement time" and "transmission time" as two separate entities, which allows in-application queuing as well as solution transmission latency monitoring if desired.

When deploying units configured to transmit at regularly scheduled intervals, Iridium strongly advises that transmissions are randomized as much as possible, down to fractions of a minute. This will ensure the health of the network, improve security (transmissions not predictable) and ultimately benefit all SBD users by distributing demand for services. To optimize your transmissions, you should:

1. Avoid transmitting at the top of the second, minute, hour and day.
2. Space individual transmissions throughout the minute and ensure messages are evenly distributed over time.
3. SBD response codes should be used to identify whether a transmission has completed and its status e.g. success/fail. If the SBD session was successful, you may retransmit right away.
4. If the Iridium modem is in a tracking application with frequent mobile originated messages throughout the day, we recommend 60 seconds between transmissions.
5. Before transmitting, check for good signal quality and network availability. If the session fails (e.g. code 32), implement a retry back off scheme starting with 60 seconds. Do not continuously retry.

Be aware that traffic management will activate if you initiate an SBD session multiple times with no success, or little to no signal quality. Under such circumstances, the modem places a timer preventing any further SBD sessions for a specified duration of time – starting with fractions of a second up to a maximum of 10 minutes. See "+SBDLOE" in the AT Command guide for more information and ensure you application is properly configured to manage this.

2.2 Transmission must be disabled prior to deactivation

Please note that prior to deactivating a unit on the Iridium network, transmissions and network access requests from SBD devices must be disabled. Customers often use deactivation for temporary suspension instead of the appropriate “Active” or “Suspended” activation status. Iridium continually monitors network resources and will take steps to address this to ensure the best possible network experience.

In some cases, customers might not be able to access devices in order to disable transmissions from certain inactive SBD devices, particularly for devices located in remote or inaccessible areas. Iridium might be able to remotely disable a unit from transmitting upon request. If devices continue to utilize network resources after deactivation, Iridium will issue remote disable commands over the Iridium network that will remotely disable a device. Please note that, once a device is disabled in this manner, the only way to reactivate it is by sending a specific AT command to the device locally over the device’s AT command port. It is not possible to reactivate any Iridium device disabled in this manner over the Iridium network. Customers will need to use physical access. In some cases, this may be possible remotely if such capability to access and send commands to the Iridium devices AT port via an alternative mechanism such as cellular service or Wi-Fi has been created within your application.

2.3 Delivery of MO Messages

In the delivery of MO messages the user first clears the buffer, then frames the message and moves it to the transmit buffer of the Iridium Transceiver (i.e. Iridium 9522 series, 9601, 9602, all handsets). After the application receives the ‘OK’ response, it initiates the SBD session. The session includes acquiring the satellite, authenticating the Iridium transceiver, sending the MO messages, receiving a MT message if one is available, exchanging status information and performing the final ACK / NAK.

If the MO status response codes indicate a success, the MO message was delivered successfully to the GSS. If the response codes indicate a failed transmission (e.g. RF link drop, inter-satellite handoff, etc), the message remains in the transmit buffer and the user must resend it. The message is either successfully delivered to the GSS or remains in the transmit buffer, but it is not ‘lost’.

Once the MO message arrives at the GSS, it is passed to either the email or Direct IP servers for delivery. Once the message is posted to the email, Iridium has no control over the delivery. With the Direct IP, the connection to the destination server is opened, the message sent to the destination, and the connection is closed. This is a very high reliability delivery method.

If the MO messages cannot be delivered, usually because the destination server is offline and the GSS will queue them until the server comes back on line. The system is configured to hold 10,000 messages per application at the GSS.

For DirectIP MO messages, when sizing network capacity, the general guideline is that one IP address: port pair can support a delivery rate of 100 messages per minute from the Iridium server to the partner server. A partner may configure the number of IP address: port pairs based on expected peath throughput levels for any given day.

2.1.1 9601 MOMSN Single Transmitter

The 9601 & 9602 were designed with only one transmitter, so there will be instances when an SBD call is not completed due to the call dropping as it moves from one satellite beam to another beam. Partners may see duplicate MOMSN numbers being created due to this beam handoff phenomenon.

What is happening is that the SBD-MO message is received at the Iridium gateway, and as the acknowledgement is sent back to the remote device, the connection gets dropped. The remote device never receives the acknowledgement and retransmits the same message using the same MOMSN.

2.0 Delivery of MT Messages

In the delivery of MT messages the vendor application creates a message and sends it to the GSS; either via email or the Direct IP connection. The GSS sends a receipt to the vendor application indicating the GSS received the MT message and queued for delivery to the Iridium transceiver.

The GSS does not automatically attempt to deliver the MT messages. Since the SBD is a success based protocol, the GSS will not send the MT message unless the destination is ready to receive it. The destination Iridium transceiver must therefore request delivery of the queued MT message. This is done by initiating a SBD session. The session can be either a valid MO message or a 'mailbox check.' A 'mailbox check' is a MO message with a 0-byte message payload.

If the Iridium transceiver is configured to receive the automatic Ring Alerts, and there is a line of sight between the unit and the satellite, the GSS will send the RA to the Iridium 9602 notifying the device that a message is waiting to be retrieved.

If the Iridium transceiver is powered off or not in view of the satellite, the MT messages remains queued at the GSS. The GSS can queue up to 50 MT messages for each IMEI. A MT message can remain queued at the GSS for 5 days from receipt at the gateway. If a MT message is not retrieved by the application within this 5 day window, the daily maintenance program at the GSS purges the queue for this IMEI. The message is not 'lost' but remains queued at the GSS for up to 5 days.

For DirectIP MT messages, all partners should immediately disconnect their socket connection after the data has been transferred and an acknowledgement is received from the Iridium server. Additionally, there should be a timeout period of 5 seconds once the partner server had sent the SBD payload data to the Iridium server, and is awaiting a response back from the Iridium server. All partners need to configure their server to allow a maximum of 20 simultaneous connections to the Iridium server. This will ensure access for all partners.

3.0 Power On/Off

The Iridium Subscriber Unit (ISU) should be powered on / off in a prescribed sequence. Both the Iridium 9601 and Iridium 9602 have an ON/OFF pin to control the power on off sequence. Assuming that power is supplied to the ISU when power is applied to the pin, the ISU boots up, and when power is removed it executes an orderly shutdown. For the Iridium 9601 this is pin 7 and the Iridium 9602 it is pin 5. The device is ON if 2.0 V or more is applied and is OFF if 0.5V or less.

Removing power from the ISU while effectively powering down of the ISU, is not a recommended practice since it does not guarantee the buffers are flushed and the variables are written to non-volatile memory. If the user wants to power down the ISU by removing power, they should first issue the AT*F command. This command flushes all pending writes to non-volatile memory, shuts down the radio, and prepares the ISU to be powered down.

The ISU can then be powered down by removing power or de-asserting the ON/OFF line.

At power ON, the ISU executes a sequence of power on and memory tests. Interrupting this sequence can possibly cause problems with the ISU. Logic has been added to increase the robustness of operation and minimize the possibility of memory corruption; however it is recommended that the application wait at least 2 seconds between initiating a power ON sequence and powering OFF the unit.

4.0 Automatic Ring Alert

The Automatic Ring Alert feature notifies the ISU when a MT-SBD message is queued for this IMEI. When the ISU receives the Ring Alert, a number of unsolicited events occur; if the device is in verbose mode, the ISU sends the ASCII string SBDRING across the data port to the field application, if it is not in verbose mode, the ISU sends the string 126. Also the RI bit (9601 pin 24, 9602 pin 19) is asserted and the Ring Alert bit in the ISU is set.

These events notify the application that a MT-SBD message is waiting and the field application can then send a +SBDIXA ‘mailbox check’ to retrieve the message. If the application does not reply with a +SBDIXA ‘mailbox check’ within 20 seconds, the gateway sends a second Ring Alert to the ISU. If there is still no response, the Ring Alerts are cancelled and the ISU will not receive another Ring Alert until another MT-SBD is queued for this device or the Host ‘forces’ a Ring Alert using the Direct IP.

The forced ring alert feature consumes Iridium network resources. Currently there is not charge for the use of a forced ring alert; however unreasonable use of the feature could force Iridium to evaluate this position. In order to use the Ring Alert feature, a few steps must be followed:

- First, the Ring Alert option must be selected in the provisioning for this IMEI. This is done by the user from the SPNet tool.
- Second, the application must configure the ISU to listen for the Ring Alert signal using the +SBDMTA command.
- Lastly, the ISU must be ‘attached’ to the gateway. This may be done with the +SBDREG command or initiating a SBD session with the +SBDIX command.

5.0 Attaching an ISU to the Gateway

The ‘attach’ process performs two functions; it indicates to the gateway that the ISU is configured to receive the Ring Alert and it updates the geo-location of the ISU on the gateway so the Ring Alert signal can be routed to the device. The ‘attach’ can be accomplished in two ways.

+SBDREG

The +SBDREG command ‘attaches’ the ISU to the gateway so it can receive the Ring Alert. When used, it notifies the gateway this IMEI is configured to receive the Ring Alert and updates the geo-location data. This command only needs to be executed one time. Once a device is attached, it remains attached until it is ‘detached’ by the field application. This is done by issuing the +SDBDET detach command or using the +SBDI command to initiate a SBD session.

+SBDIX

Every time the application issues the +SBDIX command the gateway attempts to 'attach' the device. For a fixed site or a device that operates in a limited geography, this will keep the device 'attached'. This mitigates the need for using the +SBDREG command.

+SBDNET

This command 'detaches' a device from the gateway so it no longer can receive the automatic Ring Alerts, and also returns status information to the ISU which indicates if an MT-SBD message is queued at the gateway from this device.

5.1 Invalid geo-location Auto re-attach / SBDAREG

The gateway relies on a current geo-location to determine which spot beams to route the Ring Alert to the device. If the field application is mobile, it may move outside of the ring alert radius without updating its geo-location by a +SBDIX command. When this occurs the mobile device will not receive the Ring Alert from the gateway. This can be addressed in two ways; periodically issue a +SBDIX command to re-attach or use the +SBDAREG command. NOTE: the +SBDIX is a billable event based on the number of bytes sent (a zero byte message is considered a mailbox check if there is no MT message awaiting delivery.

When run, the +SBDAREG performs a passive geo-location which estimates the distance the ISU has moved since the last attach. If this indicates the device may have moved beyond the Ring Alert radius, it automatically re-attaches the device. The application does not need to monitor the frequency of MO-SBD messages or issues periodic +SBDAREG commands.
The +SBDAREG works if the device is power cycled and moved. The caveat is that when the device is powered on, the calculation may take minutes to determine the geo-location and re-attach. The +SBDAREG command is local to the ISU and must be issued after the ISU has been successfully attached to the gateway. It is NOT an alternative to the +SBDREG command, it is a complement.

To use the +SBDAREG

- Attach the ISU to the gateway. This may be done with the +SBDREG command or initiating a SBD session with the +SBDIX command.
- Check that the response code indicates as successful 'attach'
- Issue AT+SBDAREG <mode>

6.0 Recognizing and Responding to the Ring Alert

The field application is configured to look for the unsolicited ASCII string SBDRING or 126 to indicate that the Ring Alert was received by the ISU. The RI pin, 17 on the 9601 and pin 12 on the 9602, is also is also asserted on the ISU when the Ring Alert is received.

There are two additional commands available to the developer for checking the status of the Ring Alert pin. These are the +CRIS, Ring Indication Status and the +SBDSX, Status Extended commands.

+CRIS.

The +CRIS returns the reason for the most recent assertion of the Ring Indicate signal. There are separate indications for telephony and SBD. For the Iridium 9601 / 9602, the SBD indicator is the only valid response.

+SBDSX

The +SBDSX returns the status of the last successful SBD session and the Ring Alert flag. The Ring Alert flag indicates whether an SBD ring alert has been received and still needs to be answered. This flag is cleared by a successful SBD session, including 'mailbox checks'.

If the designer does not wish to handle the unsolicited ASCII strings, the field application can periodically check the Ring Alert status with either of these commands instead to determine if a Ring Alert was received.

Once the field application has determined that the ISU received a Ring Alert, it can initiate a SBD session to retrieve the queued message. Typically this is accomplished with a 'mailbox check' which is a MO-SBD message with a 0-byte payload. The MT-SBD message waiting at the gateway is delivered as part of the SBD session. A MO-SBD message with a valid payload also retrieves the pending message.

The application should use the +SBDIXA command when responding to the Ring Alert.

7.0 Network Satellite Availability

Iridium operates on the principle of line of sight communications and requires that the antenna maintain a clear view of the satellite. Since the Iridium satellites operate in low earth orbits, this view may at times be obstructed. The ISU contains features that indicate to the application that a satellite is within view of the antenna.

These are the Network Available pin, +CSQ / +CSQF commands and +CIER / CIEV command

7.1 Network Available pin

The Network Available pin, 9601 / pin 24, 9602 / pin 19, is asserted when the satellite is within view of the device and the device is powered to receive a signal from the satellite. (The pin is not asserted if the device is powered off). The application board can be designed to make use of this input.

7.2 +CSQ / +CSQF commands

These commands return the Relative Signal Strength Indicator value to the application. The commands return a value between 0 and 5. The value indicates strength of the signal relative to the noise floor. A value of 0 indicates no discernable signal and the communications will not work. A value of 1 is the minimum signal strength required to transmit. Every incremental value is an additional 2 dB of margin. For example; 2 is + 2 dB, 3 +4 dB, 5 +8 dB.

The +CSQ results are not 'instantaneous' and the calculation may take seconds. The +CSQF command immediately returns the results of the last RSSI calculation to the user. The user must keep in mind this value may be 'old', perhaps 15 seconds.

7.3 +CIER / CIEV command

This command enables 'Indicator Event Reporting' which sends the unsolicited +CIEV result codes to the application. The command affects two parameters; the RSSI value and the Network Availability. When the parameter is enabled, the ISU sends the new value to the field application. This is an unsolicited response and is delivered as long as the data port to the ISU is available.

For the signal quality, it returns the latest RSSI value; 0 to 5. For the network, 'service availability' the ISU returns a 0 or 1. The +CIEV, is the unsolicited text string returned with the +CIER value.

8.0 Initiating SBD Session

There are three commands available for initiating a SBD session: +SBDI, +SBDIX and +SBDIXA.

8.1 +SBDI

The +SBDI is the legacy command from the initial release of the SBD service. It can be used for sending SBD messages but in the current system design, there are a couple drawbacks to using this command. The +SBDI will detach the ISU from the gateway. If the application uses, or intends to use, automatic Ring Alert feature, the +SBDI command cannot be used. Also, the status response codes from the +SBDI command are limited and not very useful in diagnosing possible connectivity problems. Iridium recommends using the +SBDIX command rather than the +SBDI.

8.2 +SBDIX

The +SBDIX command is the recommended command for initiating a SBD session. It ensures the ISU won't become detached inadvertently; it maintains the current geo-location for the RA and provides a more extensive set of response codes.

8.3 +SBDIXA

If the ISU is configured to receive the automatic Ring Alert, and the device is attached to the gateway, when the Host sends a MT-SBD message a RA is sent as the message is queued. If the field application does not respond to the RA within 20 seconds, a second RA is sent to the ISU. If the application is initiating a SBD session in response to the RA, it should use the +SBDIXA command. The +SBDIXA command functions the same, but it cancels the second RA. This prevents a possible race where the gateway would send a RA after the message has been retrieved.

9.0 Interpreting Command Response Codes

Each AT command returns to the application a result code that indicates the disposition of the command. Depending on the command, the codes may indicate status, condition or other related information. It is important to program the application to interpret these commands and properly execute logic based on these results.

Occasionally, a new command is introduced which provide additional features and may be used in place of exiting commands, such as +SBDIX and +SBDI. The +SBDIX can be used in place of the +SBDI, and is recommended, however, the response codes for the commands are different. Just replacing the one command with the other and not modifying how the codes are interpreted can introduce a major bug.

When a command is used, check the possible response codes and how to interpret them.

10.0 Adaptive Retry

There are a variety of reasons why a SBD message may not get through from the ISU to the satellite. Since this is a line of sight system, the most obvious cause of a link failure is an obstruction. However, it can be due to inter-satellite handoff or contention for satellite resources. The response codes indicate that the message failed, but do not always give a precise reason.

When a SBD session fails, the exception logic in the application should determine what action to take. Typically if a session fails once or twice, the application immediately initiates another session. If the resends fail beyond this, and a satellite is in view, there may be an issue with contention for satellite resources. In this case, it is better to incrementally adjust the time interval between the resend attempts.

A suggested retry scheme might be:

Initiate SBD session
If that fails attempt resend within a random time of 0-5 seconds (2 x)
If still unsuccessful wait a random time of 0-30 before attempting a resend (2X)
If these attempts fail, increment the delay to 5 minutes.

This logic should cover almost any anomaly with the network.

11.0 Features Not Supported on Iridium SBD Service

11.1 Data After Voice

Data after voice is a feature that is technically possible on the Iridium network. However, Iridium partners are advised that this feature is not supported by Iridium. Partners will not find any reference to it on our public website as Iridium does not offer any type of troubleshooting or support for thi service. Furthermore, future modifications to gateway network elements or the satellite constellation could unexpectedly and permanently render DAV inoperable.

12.0 Frequently Asked Questions

- What is the Iridium source IP address that Mobile Originated deliveries will come from
    - 12.47.179.11
- What is the Iridium domain name for DirectIP Mobile Terminated messages:
    - directip.sbd.iridium.com / port 10800
- What is the current policy regarding DirectIP Mobile Originated TimeToLive setting:
    - TimeToLive is 12hours
- What is the Iridium Mobile Terminated queue policy, before MT messages are purged;
    - MobileTerminated messages that are ‘queued’ for 5 days – (all messages for the destination will be purged at this time)
- Maximum # of Mobile Terminated messages for a single IMEI:
    - Max. of 50 messages per IMEI

- For SBD DirectIP Mobile Terminated, does the customer need to inform Iridium of the source IP address that will be utilized?

    - Yes, the source IP address that will be utilized to connect to the Iridium gateway needs to be included within the Iridium network firewalls, to allow for successful connection.. This request for DMT access needs to be sent to the partners Iridium Account Manager.

- What happens if the host server is not available to receive messages?
    - MO-SBD messages are queued at the GSS. The GSS can store 10,000 messages per server application. If the number of MO-SBD messages exceeds the 10,000 limit, the oldest message is discarded and the newest added to the queue. The expiry for the queued message is 12 hours. (ties in with #3)