Iridium Short Burst Data Developer Guide

IRDM-1023-UDOC-001 | v4.1 | r1C78E940B9 | 2025-OCT-07

LEGAL DISCLAIMER AND CONDITIONS OF USE

Use of the product (the "Product") described in this document (the "Document"), the information provided in this Document, and this Document itself is governed by and subject to the terms, licenses and restrictions of your Agreement with Iridium. Please review that Agreement. This Document is Iridium proprietary business information. Consistent with your Agreement with Iridium, you may not disclose this Document to others without express prior written permission from Iridium. Any violation of your Agreement's Proprietary and Confidentiality obligations shall result in remedies to the fullest extent available to Iridium at law or in equity.

Reasonable effort has been made to make the information in this Document reliable and consistent with other specifications, test measurements and other information. However, Iridium Satellite LLC 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 document. Iridium reserves the right in its sole discretion and without notice to you to change this Document and materials and/or revise this Document or withdraw it at any time. You assume any and all risks of using the Product and any information provided in this Document.

IRIDIUM MAKES NO REPRESENTATIONS, GUARANTEES, CONDITIONS OR WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, 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 THOSE ARISING FROM OR RELATED TO A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE OR ARISING FROM OR RELATED TO THE PERFORMANCE OR NONPERFORMANCE OF THE PRODUCT OR THIS DOCUMENT. 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 WARRANTY AND DOCUMENTATION FOR THE PRODUCT FAILS OF ITS ESSENTIAL PURPOSE.

IN NO EVENT SHALL IRIDIUM BE LIABLE, REGARDLESS OF LEGAL THEORY, INCLUDING WITHOUT LIMITATION CONTRACT, EXPRESS OR IMPLIED WARRANTY, STRICT LIABILITY, GROSS NEGLIGENCE OR NEGLIGENCE, FOR ANY DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, IF ANY. NOR SHALL IRIDIUM BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, 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 PRODUCT (INCLUDING HARDWARE, SOFTWARE AND/OR FIRMWARE) AND/OR THE IRIDIUM SATELLITE SERVICES, OR ARISING OUT OF OR IN CONNECTION WITH THE ABILITY OR INABILITY TO USE THE PRODUCT OR ANY OTHER IRIDIUM PRODUCTS (INCLUDING HARDWARE, SOFTWARE AND/OR FIRMWARE) AND/OR THE IRIDIUM SATELLITE SERVICES TO THE FULLEST EXTENT THESE DAMAGES MAY BE DISCLAIMED BY LAW AND WHETHER IRIDIUM WAS 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.

LIMITED LICENSE TO SOFTWARE/FIRMWARE

The Product may contain software, including firmware and software made available by one or more third parties (the "Software.") To the extent it does, each such item of software is subject to the applicable terms and conditions (the "Software Terms") available at https://www.iridium.com/resources/?fwp_resource_categories=legal-notice. Do not use the Product until you have carefully read the Software Terms. Do not use the Product if you do not wish to agree to the Software Terms. Your use of the Product constitutes your acceptance of all of the Software Terms. Without limiting the foregoing, if you do not agree to the Software Terms, you are not granted any license or rights whatsoever to use the software contained on the Product.

EXPORT COMPLIANCE INFORMATION

This document or item contains information subject to the Export Administration Regulations (EAR) (15 CFR 730-774). It may not be exported, disclosed, or transferred to any foreign person without the applicable prior authorization of the U.S. Department of Commerce. Violations may result in civil or criminal penalties. ECCN: 5E991

© Iridium Satellite LLC 2003-2025

Revision History

Version	Date	Description
1.0	01-JUN-2003	First Commercial Release
1.1	24-AUG-2005	Changes Summary: • Updated Network Features: ◦ ISU-ISU SBD ◦ Optional reporting of geographic location on email messages ◦ MTMSN unique for each ISU ◦ Session status fields generated by the Iridium Gateway • Additional Documentation ◦ Multiple MT-SBD destinations in a single email ◦ Multiple MT-SBD payloads in a single email Incorporation of other documentation. ◦ SBD Troubleshooting Guide • Removal of generic 9522 information
1.2	10-FEB-2006	Updated to reflect 9601 SBD Transceiver information and updates from network updates to the Iridium Gateway to Version 4.1
1.2.1	23-FEB-2006	Updated to correct typographical error in 2.1
2.0	20-MAR-2007	Changes Summary: • Updated to include IP Socket Information • Updated to include SBD Security Information • Updated to include features up to and including Iridium Gateway Version 4.2 Removed AT Command Descriptions

Version	Date	Description
2.01	05-DEC-2007	Changes Summary: • Updates to correct typographical errors and clarifications. • No functionality changes implemented. • Minor feature additions • Revised recommendations and new requirements in Section 6 Specific Changes: • New addition: 3.4 Permitted Email address Formats • New addition: 3.5 Bit Bucket for MO-SBD Messages • 4.1.4.2 Clarifications on SBD Ring Alerts • Table 5-6 Values correct for "Overall Message length", and "MT Confirmation Header Message Length". Removal of "MT Confirmation IEI" and "MT Confirmation Length" Fields. • Table 5-7 - Corrected to show correct table names. • 5.4.2.7 Clarification of epoch reference • Section 6.0 significantly updated and re-titled from "Optimal Message Size Selection" to "practical Considerations and Requirements for SBD Application Design and Solution Certification."
2.2	09-JUN-2008	Changes Summary: • Updated to include multiple DirectIP Destinations • Updated to include filtering of Mt-SBD Message Originators
2.3	15-JUL-2010	Changes Summary: • Updated to reflect 9602 SBD Transceiver and 9522B Transceiver • Update to existing sections; 2.1, 2.2, 3.1, 4.1.4, 5.1.2.1, 5.1.3, 5.1.3, 5.2.2 • Update to existing Tables: 0-2, Table 3-1, • New addition; Section 3.5
2.3.1	01-OCT-2010	Changes Summary: • Updates section 2.1, 3.1,3.2, 4.1.4,5.1.2.1 • Update to tables 3-3, 3-4

Version	Date	Description
3.0	01-JAN-2012	Changes Summary: • Complete Reorganization of document • Inclusion of SBD 5.3 features
3.1	01-OCT-2012	Corrected references in section 6.2.7
3.2	01-OCT-2017	Changes Summary: • Updated SBD transceivers • Updated MT changes for IWS, SPnet, Russia gateway restrictions • Added transmission intervals best practices
4.1	07-OCT-2025	Changes Summary: • Updated content throughout the guide • Updated the list of transceivers • Added SBD Transceiver Message Sizes and the latest firmware • Added Best Practices for SBD Transmissions • Rearranged the document structure by service type • Added an Iridium Time Re-Epoch Advisory • Added Dual Mode Operation for SG25001 or later • Updated formatting and added references to the new Iridium 9602 and 9603 AT Command Reference Guide. • Issued document number IRDM-1023-UDOC-001.

Documentation Feedback

To provide feedback on this document, open a ticket in the Partner Support portal (Iridium Service Desk) and under Component select Document Feedback.

Table of Contents

Revision History . . . 2
Documentation Feedback . . . 4
1. Introduction . . . 7
1.1. Purpose . . . 7
1.2. Scope . . . 7
1.3. Overview of Iridium Satellite Network for Short Burst Data . . . 7
2. Best Practices for SBD Transmissions . . . 11
3. Optimal Message Size Selection . . . 12
3.1. Minimum Billable Message Size . . . 12
3.2. Message Segmentation . . . 12
4. SBD Messaging . . . 13
4.1. SBD Sessions (+SBDIX) . . . 15
4.2. Iridium Gateway MO & MT Queues . . . 17
4.3. Signal Strength (+CSQ) . . . 17
4.4. Signal Monitoring (+CIER) . . . 18
4.5. MO & MT Buffers . . . 18
4.6. Ring Alerts . . . 25
4.7. Traffic Management . . . 26
4.8. Retrieving Transceiver Characteristics . . . 27
4.9. Sample Field Application . . . 30
5. Direct Internet Protocol Socket "DirectIP" Interface . . . 31
5.1. DirectIP Message Delivery . . . 32
5.2. Vendor Application DirectIP Server/Client Requirements . . . 33
5.3. DirectIP Overall Message Structure . . . 34
6. Email Description . . . 51
6.1. Email MO . . . 51
6.2. Email MT . . . 54
7. ISU-ISU Messages . . . 58
8. Iridium Short Burst Data Service Security Features . . . 60
8.1. Authentication Security . . . 60
8.2. Iridium Channel Security . . . 60
8.3. L-Band Channel Security . . . 62
8.4. K-Band Channel Security . . . 62
8.5. Gateway to Vendor Application . . . 62
8.6. Additional Considerations . . . 63
9. Basic Troubleshooting Steps . . . 64

9.1. Transmissions from Deactivated Units . . . 65
10. Iridium Time Re-Epoch Advisory . . . 66
10.1. Iridium Half-Time . . . 66
11. Dual Mode Operation: . . . 67
Appendix A: Definitions, Acronyms, and Abbreviations . . . 68
Referenced Documents . . . 70
Email RFC Compliance . . . 71

1. Introduction

1.1. Purpose

The purpose of this document is to provide technical and operational information sufficient for an Iridium Value Added Reseller or Value Added Manufacturer to be able to develop an integrated data application that utilizes the Iridium Short Burst Data® Service (SBD). Additional information may be required by the developer for the AT Commands to be utilized with the transceiver selected for use with SBD.

An overview of the satellite network is provided as well as descriptions of the transceiver equipment and the end to end communications protocol for SBD. This document is intended for use by technical personnel and assumes a reasonable level of technical skill and familiarity with satellite and/or wireless data applications.

1.2. Scope

This document provides an explanation of:

1. How the Mobile Originated and Mobile Terminated SBD protocol works
2. Specific SBD related AT commands and responses as it relates to Mobile Originated and Mobile Terminated SBD messages
3. Interface requirements between the Iridium Gateway and the Vendor Application

Additional documents are referenced which provide more specific detail on certain topics and these are listed in the Referenced Documents section of this document. This document does not specifically define the provisioning process, although it does reference it. This document assumes a working knowledge of the Iridium® satellite system.

1.3. Overview of Iridium Satellite Network for Short Burst Data

Iridium's Short Burst Data Service (SBD) is a simple and efficient satellite network transport capability to transmit short data messages between field equipment and a centralized host computing system. The maximum Mobile Originated (MO) SBD and Mobile Terminated (MT) SBD message sizes are transceiver specific and are described in Section 1.3.1, "Transceiver Overview" of this document.

NOTE	A zero (0) byte MO SBD message is referred to as a "Mailbox Check."

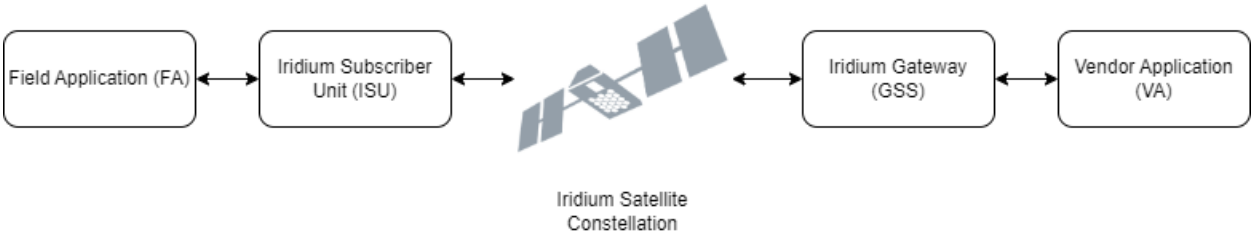


Figure 1-1 Short Burst Data Architecture

The primary elements of the end-to-end SBD architecture are shown in Figure 1-1 above. Further details can be found in the table below:

Table 1-1 SBD Architecture Elements

Element	Description
Field Application (FA)	The hardware and software that is configured by the VAR for specific applications such as collecting and transmitting GPS location information
Iridium Subscriber Unit (ISU)	An Iridium L-Band Transceiver (LBT) with the SBD feature available in firmware and the service activated on the Iridium network
Iridium satellite constellation	Transmits messages to and from the ISU
Gateway SBD Subsystem (Iridium Gateway, GSS)	Responsible for storing and forwarding messages from the ISU to the Vendor Application and storing messages from the Vendor Application to forward to the ISU
Vendor Application (VA)	Sends and receives messages via email, DirectIP socket or Iridium Cloud Connect

When transmitting SBD messages, Iridium transceivers initiate a connection with the constellation and transmit. These connections are bidirectional - meaning that the ISU will simultaneously transmit an MO message and receive an MT message (if there are any waiting in the queue) during each SBD session. The Iridium Gateway then passes any transmitted MO messages to the appropriate delivery destination. For MT messages, the message is sent to the Gateway and then queued for pickup by the appropriate transceiver. Iridium has three services available for sending and receiving SBD messages from the Gateway:

- **Email** - Messages are sent and received by an email address. This is the most inefficient method of transmitting messages and is typically only used for testing purposes.
- **DirectIP** - Messages are transmitted directly to/from an IP address connected to a server built and maintained by the partner. IP addresses must be whitelisted in the Iridium Gateway before they can be utilized to send/receive messages.
- **Iridium Cloud Connect SBD** - DirectIP utilizing Amazon Web Services (AWS) services. Messages are sent between the Gateway and AWS Simple Queue Service via a DirectIP connection
- **ISU-ISU** - Messages are sent directly from one ISU to another

The vendor application (VA) is responsible for sending MT messages and receiving MO messages via these services. Requirements for vendor applications can be found in Section 5.2 Vendor Application DirectIP Server/Client Requirements. Each ISU can have up to five delivery destinations. Every MO message transmitted by the ISU will be sent to all five destinations. These destinations can be DirectIP IP address/port pairs, email addresses or the IMEI of another Iridium device. The delivery address for each IMEI can be changed online by the VAR using the Iridium SPNet provisioning tool.

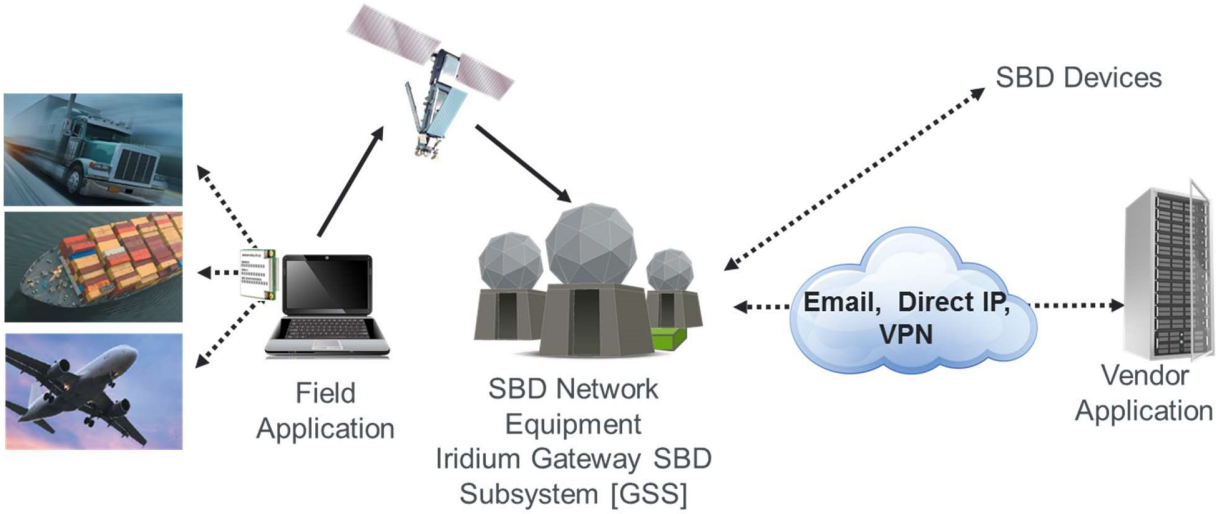


Figure 1-2 SBD System Architecture

The interface between the FA and the ISU is a serial connection with extended proprietary AT commands. This interface is used to load and retrieve messages between the ISU and the Field Application. This document outlines recommended commands for basic operation of SBD capable Iridium transceivers. A full list of available AT commands can be found in the *Iridium AT Command Reference Guide*.

1.3.1. Transceiver Overview

The following Iridium transceivers are capable of Short Burst Data Service:



9602



9603



9523

NOTE Transceivers depicted above are not to scale.

Developers should consult the appropriate developers guide document for their transceiver hardware.

1.3.1.1. Transceiver Message Sizes

Maximum message sizes are listed below for SBD-capable transceivers.

Table 1-2 SBD Transceiver Message Sizes

Transceiver	Maximum MO Message Size (Bytes)	Maximum MT Message Size (Bytes)
9523	1960	1890
9602	340	270
9603	340	270

1.3.1.2. Transceiver Firmware

Minimum firmware versions are listed below for SBD-capable transceivers. The 9523 is voice-capable and requires a SIM card. The 9602 and 9603 do not require SIM cards. **For best performance, transceiver firmware should be kept up to date.**

Table 1-3 SBD Transceiver Firmware

Transceiver	Expected Firmware Revision	Requires Valid SIM Card?
9523	DB24002	Yes
9602	SG25001	No
9503	SG25001	No

NOTE Firmware revisions may have changed since this document was last updated. The latest firmware can be downloaded from the Iridium For Partners (IFP) website. Iridium will notify partners when new firmware is released.

2. Best Practices for SBD Transmissions

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 (TX not predictable) and ultimately benefit all SBD users. To optimize your transmissions, you should:

- Avoid transmitting at the top of the second, minute, hour and day.
- Space individual transmissions throughout the minute and ensure messages are evenly distributed over time.
- 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.
- If the Iridium transceiver is in a tracking application with frequent mobile originated messages throughout the day, we recommend 60 seconds between transmissions.
- 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.

Table 2-1 Best Practices Implementation Examples

Best Practices Implementation Examples	
Not Best Practices	Best Practices
MO1 Transmit time: 00:00:00 Immediate retry if failed	MO1 Transmit time: 01:10:10 60+ second delay if failed
MO2 Transmit time: 00:01:00 Immediate retry if failed	MO2 Transmit time: 01:11:05 60+ second delay if failed

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 transceiver 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 *Iridium AT Command Reference Guide* for more information and ensure that your application is properly configured to manage this.

3. Optimal Message Size Selection

3.1. Minimum Billable Message Size

Developers should consider minimum billable message size of the service plan that the ISU will be activated with on the Iridium® network. For example, for a minimum billable message size of 10 bytes, any message sent with less than 10 bytes will be billed at 10 bytes regardless of the actual number of bytes sent below 10. All messages over 10 bytes will be billed at the exact number of bytes transmitted.

3.2. Message Segmentation

Each type of message whether MO or MT is broken into segments for actual transmission. The length of the segment relative to the absolute message length depends on whether it is a MO or MT message. Between each segment additional signaling and network overhead occurs. If optimizing for minimal latency or power consumption then the minimal number of message segments should be used.

For mobile originated (MO) messages, the first user segment will be 70 bytes. Following segments will be 135 bytes each. For example, for a 1960 byte MO message there will be one segment of 70 bytes followed by 14 segments of 135 bytes each. Mobile terminated (MT) message segments are 135 bytes each. For example, for a 71 byte MT message one segment will be used.

Table 3-1 SBD Message Segment Sizes

Message Type	Segment	Segment Size
Mobile Originated	First Segment	70 Bytes
	Subsequent Segments	135 Bytes
Mobile Terminated	All segments	135 Bytes

4. SBD Messaging

To send and receive messages, the ISU must initiate an SBD session. SBD sessions are two-way: they simultaneously pick up any queued MT messages and send MO messages. Each session handles a single transmission, or a single MO and MT message. Mailbox checks, i.e. SBD sessions that check for queued MTs without sending out an MO message, are identical to typical SBD sessions but have an empty MO payload. This is achieved by starting an SBD session while the MO buffer is empty.

To complete an SBD session:

- **+SBDS:** Optional - check status of MO and MT buffers
- **+SBDWB:** Load binary data into the MO buffer (or erase MO buffer with **+SBDD0** if performing a mailbox check) Optionally, **+SBDWT** can be used to load text (i.e. ASCII characters) into the MO buffer
- **+CSQ:** Check signal strength with - for best results, signal strength should be 2 or higher
- **+SBDIX:** Start an SBD session
- **+SBDRT/+SBDRB:** If any MT was picked up from the gateway, retrieve MT data from the MT buffer
- **+SBDD0:** Erase MO buffer

More details for each of these commands can be found in the *Iridium 9602 and 9603 AT Command Reference Guide*.

Table 4-1 Recommended AT Command Sequence for SBD Sessions

Recommended AT Command Sequence for SBD Sessions	
Command	**Description**
AT+SBDS	Return current state of MO and MT buffers
+SBDS: <MO flag>,<MOMSN>,<MT flag>,<MTMSN> OK	
AT+CSQ	Check signal strength (should be 3 bars or greater)
+CSQ: <Signal Strength> OK	
AT+SBDWB=<msg length>	Instruct ISU to write a message to the MO buffer (NOTE: size of message must match)
READY (binary transfer of MO message here) 0 OK	
AT+SBDIX	Start SBD session and send the message in the MO buffer
+SBDIX: <MO status>,<MOMSN>,<MT status>,<MTMSN>,<MT length>,<MT queued> OK	
AT+SBDRT/+SBDRB	Return contents of MT buffer. +SBDRT prints data to the terminal and +SBDRB will send data directly to the FA over the serial connection.
+SBDRT: <buffer contents> OK	
AT+SBDD0	Clear MO buffer
0 OK	

4.1. SBD Sessions (+SBDIX)

+SBDIX is used to conduct an SBD session with the Iridium Gateway. Messages are transferred between the ISU and the Iridium Gateway using a reliable transport mechanism that ensures the message is delivered error free. If the ISU was not able to send or receive messages, an indication is passed to the FA via the serial interface. The +SBDIX command returns several values indicating the status of the associated SBD session:

- MO Status- Status of the MO message or mailbox check
- MOMSN - MO message number; AKA the number of messages that has been sent from this transceiver. This value is incremented every time an SBD session is completed, even if the MO payload was empty.
- MT Status - Status of any MT message picked up from the Gateway
- MTMSN - MT message number.
- MT Length - Length (in bytes) of the MT message received from the Gateway.
- MT Queued - Number of MT messages queued at the Gateway

4.1.1. MO Status Flag

Status of the MO message indicates if an MO message was successfully sent to the Gateway. If the SBD session was able to complete, the MO flag will be 0. Common MO status response codes are included in the following table.

Table 4-2 MO Status Flag Response Codes

Mo Status Flag Response Codes	
Response Code	Description
0	MO message, if any, transferred successfully
2	MO message, if any, transferred successfully, but the requested Location Update was not accepted
18	Connection lost (RF drop)
32	No network service, unable to initiate call
38	Try later, traffic management period (see 4.7 Traffic Management)

For a full description of +SBDIX response codes, see +SBDIX in the *Iridium AT Command Reference Guide*.

4.1.2. MT Status Flag

Status of the MT message indicates if an MT was picked up from the Gateway and if that transaction was successful. If there was no MT message to transfer, MT status and all associated MT values (MTMSN, MT Length, MT Queued) will be 0. These MT values will only populate if an MT was successfully transferred from the Gateway. If an MT was successfully transferred, MT status will be 1. Possible MT status codes are listed in the following table.

Table 4-3 MT Status Flag Response Codes

MT Status Flag Response Codes	
Response Code	**Description**
0	No MT message to receive from the GSS
1	MT message successfully received from the GSS
2	Error occurred while attempting to perform a mailbox check or receive a message from the GSS

4.1.3. Sample +SBDIX Responses

Table 4-4 Sample SBDIX Response - MO Only

Sample SBDIX Response - MO Only		
+SBDIX: 0,149,0,0,0,0		
0	MO Status	MO message was successfully sent to the Gateway.
149	MOMSN	149th message sent from this transceiver
0	MT Status	No MT message to receive
0	MTMSN	No MT message to receive
0	MT Length	No MT message to receive
0	MT Queued	No MT messages queued at the Gateway

Table 4-5 Sample SBDIX Response - MO & MT

Sample SBDIX Response - MO & MT		
+SBDIX: 0,150,1,65,53,6		
0	MO Status	MO message was successfully sent to the Gateway.
150	MOMSN	149th message sent from this transceiver
1	MT Status	MT message successfully received from the Gateway
65	MTMSN	65th message received by this transceiver

Sample SBDIX Response - MO & MT		
53	MT Length	MT 65 contains 53 bytes
6	MT Queued	6 MT messages remaining in queue at the Gateway

4.2. Iridium Gateway MO & MT Queues

The Iridium Gateway has queues for both MO and MT messages. Each ISU has its own dedicated queue. The MO queue holds up to 10,000 messages - this is mostly relevant to VAMs receiving large volumes of data via DirectIP (see Section 5.2 Vendor Application DirectIP Server/Client Requirements for more information.) The MT queue holds up to 50 messages. These messages expire after 5 days. If the queue is full when the Gateway receives a new message, the oldest MT message will be deleted to make room for the new message.

Table 4-6 Iridium Gateway Queue Sizes

Iridium Gateway Queue Sizes			
MO		**MT**	
Size	Timeout	Size	Timeout
10,000	DirectIP - 12hrs	50	7 days (Email & DirectIP)
	Email - 5 days		

4.3. Signal Strength (+CSQ)

Signal strength (RSSI) can be checked with +CSQ. Signal strength ranges from 0 to 5 bars, where 0 is no connection and 5 is maximum signal strength. If the ISU is in the process of acquiring the system or in a satellite handoff, there may be a delay of up to 10 seconds before +CSQ returns signal strength.

Table 4-7 Signal Strength Example (+CSQ)

Signal Strength Example (+CSQ)	
AT+CSQ	Acquire signal strength
+CSQ: 5 OK	Current signal strength equivalent to 5 bars

4.4. Signal Monitoring (+CIER)

+CIER can be used to monitor several network characteristics, including signal strength. When configured correctly, +CIER will return unsolicited messages when signal strength changes. +CIER can also be used to monitor service availability and SV and beam coordinates. There is also an antenna fault flag, however as of this revision this feature has not been implemented. For more details on +CIER, please consult the appropriate section in the AT Command Guide. The example below demonstrates how to use this command to monitor signal strength.

Table 4-8 Signal Monitoring Example (+CIER)

Signal Monitoring Example (+CIER)	
AT+CIER=1,1,0,0,0	Enable signal strength reporting
OK	Command successful
+CIEV:0,5	Unsolicited message indicating signal strength - current signal strength equivalent to 5 bars

4.5. MO & MT Buffers

Each ISU is equipped with an MO and MT buffer. The MO buffer holds data waiting to be sent out during the next SBD session. The MT buffer holds the most recent MT message received by the transceiver. The MT buffer will be overwritten after every SBD session, even mailbox checks. If there is no MT to be picked up, the MT buffer will be erased. Both buffers are intended only as temporary storage, and any data in them will be erased when the transceiver shuts down.

Table 4-9 MO & MT Buffer Conditions

MO & MT Buffer Conditions	
MO Buffer	**MT Buffer**
Erased on shutdown	Erased on shutdown
Overwritten when a new MO message is loaded into the buffer	Overwritten during every SBD session - if there is no MT to receive, MT buffer is erased
Can be manually erased (+SBDD)	Can be manually erased (+SBDD)

4.5.1. Writing to the MO Buffer (+SBDWB)

+SBDWB can be used to write to the MO buffer. The length in bytes of the message being loaded into the MO buffer must be attached to the command. For example, if the message is 5 bytes long, then the command will be: AT+SBDWB=5. After sending this command, the transceiver will respond READY. The message must be transferred in binary over the serial connection - it can't be typed in directly via a terminal. The FA has 60 seconds to transfer data before the command times out. Data transferred should not exceed the maximum message size of the transceiver's MO buffer.

Table 4-10 MO Buffer Sizes

MO Buffer Sizes	
Transceiver	Maximum MO Message Size (Bytes)
9523	1960
9602	340
9603	340

A two-byte checksum must be appended to the data loaded into the MO buffer. This checksum is simply the sum of each byte in the MO message. For example:

Table 4-11 MO Message Checksum Example

MO Message Checksum Example	
Text to send	hello (in ASCII) = 68_h 65_h $6C_h$ $6C_h$ $6F_h$ (in hex)
Sum	68_h (104) + 65_h (101) + $6C_h$ (108) + $6C_h$ (108) + $6F_h$ (111) = 02_h 14_h (532)
Checksum (in hex)	02_h 14_h
Final message (in hex)	68_h 65_h $6C_h$ $6C_h$ $6F_h$ 02_h 14_h

After the data is transferred, the transceiver will return one of the following response codes:

Table 4-12 Possible SBDWB Response Codes

Possible +SBDWB Response Codes	
0	SBD message successfully written to the ISU
1	SBD message write timeout
2	SBD message checksum incorrect
3	SBD message exceeds maximum allowed size

For an example of how to load the MO buffer with a common terminal application, see the following section 4.5.1.1 Using Tera Term to Load the MO Buffer.

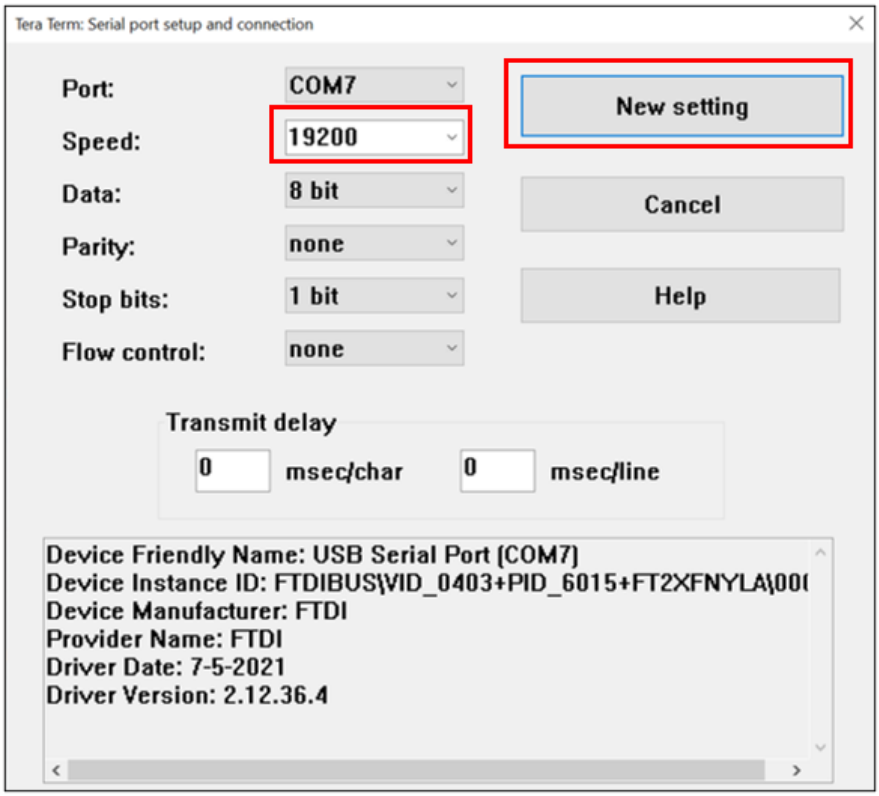
4.5.1.1. Using Tera Term to Load the MO Buffer

For testing purposes, Tera Term can be used to load data onto the MO buffer. Tera Term is an open-source terminal application that can be used to talk to connected devices via a serial port. It can be downloaded from Tera Term's GitHub page: https://teratermproject.github.io/index-en.html. Up to date documentation and instructions beyond what is included in this document can also be found on this page.

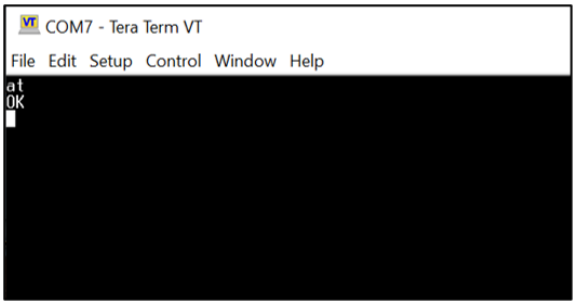
Data must be first written into a binary coded text file. This file must include the MO data and appended checksum. These files can be generated programmatically or utilizing online conversion tools (i.e. tools that take a hex input and output a binary coded file.) Since +SBDWB requires the length of data as an input, it may be useful to include the length in filenames. For example, a file containing "hello" and its checksum could be named *hello_sbdwb=5.txt*.

To load the MO buffer using Tera Term:

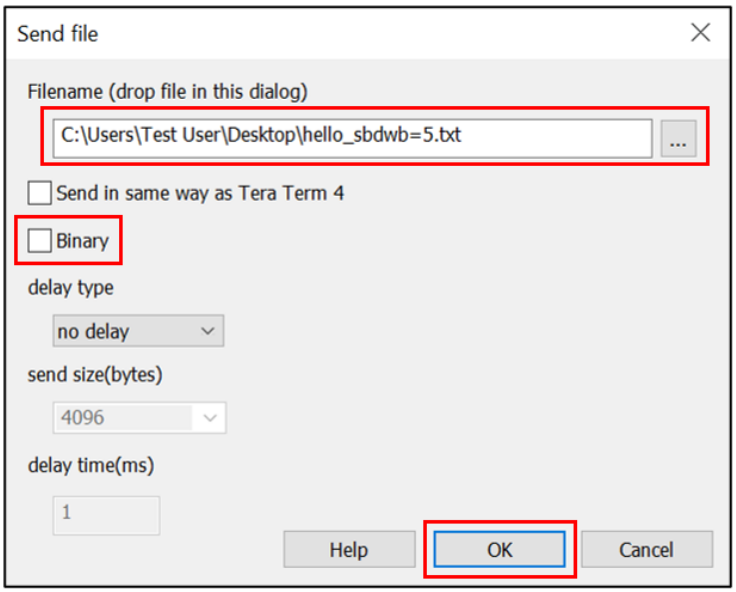
- Generate MO data text file
- Connect the transceiver to Tera Term via serial port
  - **NOTE:** Tera Term's default baud rate is 9600. This can be changed by going to Setup Serial Port, choosing 19200 from the dropdown menu, and selecting New Setting.



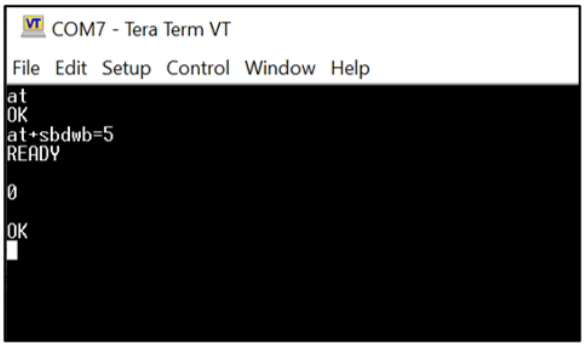
- Send AT to the transceiver to ensure the connection is active



- Send AT+SBDWB=<length> to the transceiver
- Once READY displays on the screen, go to File → Send File.
  - Select the three dots symbol to the right of the dialog box and navigate to the MO data file
  - Ensure the Binary checkbox is checked
  - Select OK to send the file



- If the transfer was successful, +SBDWB should return 0



4.5.2. Reading from the MT Buffer (+SBDRB or +SBDRT)

MT messages can be retrieved from the MT buffer using either +SBDRB or +SBDRT. +SBDRT will return the contents of the buffer in a readable format that can be viewed via terminal. +SBDRB sends the contents of the buffer directly to the FA in binary over the serial connection. +SBDRB is typically more efficient and can be used when a user-friendly output is unnecessary. +SBDRB will also return the checksum.

Table 4-13 Example MT Buffer Read (+SBDRT/RB)

Example MT Buffer Read (+SBDRT/RB)	
AT+SBDRT	AT+SBDRB
+SBDRT: hello OK	OK

4.5.3. Buffer Status Information (+SBDS)

+SBDS can be used to retrieve status information about the MT and MO buffers. +SBDS returns an MO buffer flag, the MOMSN of the next MO message, an MT buffer flag and MTMSN. For the MO flag and MT flags, 0 indicates that there is no message in the buffer, and 1 indicates that there is a message in the buffer. The MTMSN will be -1 if there is no MT message present in the buffer.

Table 4-14 SBDS Response Codes

+SBDS Response Codes	
MO Flag	Indicates the existence of an MO message in the buffer 0: No message in the buffer 1: Message in the buffer
MOMSN	MO message number for the **next** MO message
MT Flag	Indicates the existence of an MT message in the buffer 0: No message in the buffer 1: Message in the buffer
MTMSN	MT message number **NOTE:** will only be present if there is an MT message in the buffer, otherwise will be -1

4.5.3.1. Sample +SBDS Responses

Table 4-15 Sample +SBDS Response - MO Only

Sample +SBDS Response - MO Only		
+SBDS:1,151,0,-1		
1	MO Flag	MO message present in buffer
151	MOMSN	MO message number - the next MO message sent by the transceiver will be the 151st message sent from this transceiver
0	MT Flag	MT message not present in buffer
-1	MTMSN	MT message number - not provided because no MT message is present in buffer

Table 4-16 Sample +SBDS Response - MO & MT

Sample +SBDS Response - MO & MT		
+SBDS:1,151,0,-1		
1	MO Flag	MO message present in buffer
152	MOMSN	MO message number - the next MO message sent by the transceiver will be the 152st message sent from this transceiver
0	MT Flag	MT message not present in buffer
-1	MTMSN	MT message number - not provided because no MT message is present in buffer

4.5.4. Transfer MO Buffer to MT Buffer (+SBDTC)

+SBDTC can be used to transfer the contents of the MO buffer to the MT buffer. Developers can use this command to test reading and writing to the ISU without utilizing an SBD session. The command will return: "SBDTC: Outbound SBD copied to Inbound SBD: size = <data size>" if successful.

Table 4-17 Example MO Buffer to MT Buffer Transfer (+SBDTC)

Example MO Buffer to MT Buffer Transfer	
AT+SBDWB=5	Load "hello" into the MO buffer
READY (transfer "hello" in binary, with checksum) 0 OK	

Example MO Buffer to MT Buffer Transfer	
AT+SBDTC	Transfer contents of the MO buffer to the MT buffer
SBDTC: Outbound SBD copied to Inbound SBD: size = 5 OK	
AT+SBDRT	Read MT buffer
+SBDRT: hello OK	

4.5.4.1. Erase Buffer (+SBDD)

+SBDD can be used to erase the MO and/or MT buffer. To choose which buffer to erase, a deletion type should be appended to the command (i.e. to erase the MO buffer, +SBDD0 is used). Those deletion types are listed in the table below.

Table 4-18 +SBDD Deletion Types

+SBDD Deletion Types	
0	MO Buffer
1	MT Buffer
2	Both MO & MT buffer

Table 4-19 +SBDD Response Codes

+SBDD Response Codes	
0	Buffer(s) cleared successfully.
1	An error occurred while clearing the buffers.

Table 4-20 Erase MO Buffer Example (+SBDD)

Erase MO Buffer Example (+SBDD)	
AT+SBDD0	Erase MO buffer
0 OK	MO buffer successfully erased

4.6. Ring Alerts

The Iridium Gateway is not permitted to send an unsolicited MT message to any ISU as the ISU may not be ready or available to receive and acknowledge messages. However, SBD transceivers can be provisioned to enable notifications, or ring alerts, for MT messages. Recommended practice is to always enable ring alerts, but VARs may choose to disable them for certain low power applications. No additional commands are required to enable ring alerts on the transceiver itself.

The Iridium Gateway will send two ring alerts to the ISU each time an MT message is added to the queue. If the ISU doesn't respond in approximately 20 seconds after the first ring alert, a second alert is sent. However, if the ISU picks up the queued MT within 10 seconds after the first ring alert, the second one will not be sent. No further alerts will be sent if these are missed.

Ring alerts are sent as an unsolicited response on the serial connection, either SBDRING in Verbose Mode or "124" in Numeric Mode. The Ring Indicator pin (DF_RI) is also asserted. To respond to a ring alert, the FA should start a standard SBD session using +SBDIX. +SBDIXA can also be used. This command is identical in function to +SBDIX. The "A" suffix indicates to the GSS that the transceiver is responding to a ring alert and cancels the second ring alert. Signal strength should be checked before every SBD session using +CSQ.

While the transfer of MO or MT SBD messages is sent via a reliable (duplex) protocol, SBD Ring Alerts are sent on a simplex channel. If the ISU is powered off or otherwise disconnected from the network, it will not receive ring alerts. The Field Application should be built to both respond to incoming ring alerts and robust enough to handle cases where alerts might be missed. Particularly for low power applications where the transceiver may only be powered on periodically, mailbox checks should be used to check for queued MT messages. The Iridium Gateway has no knowledge of if the ISU received any given ring alert.

Table 4-21 Sample Ring Alert Response

Sample Ring Alert Response	
SBDRING	Ring alert notification
AT+SBDIX[A]	SBD Session to pick up MT message
+SBDIX: 0,151,1,66,23,5 OK	+SBDIX response: MT 66 successfully received from the Gateway

4.6.1. Automatic Registration

The +SBDIX command automatically registers the transceiver with the network before starting an SBD session. This registration must take place for the transceiver to get and transmit the current location of the ISU to the network. As previously stated, SBD messages can still be sent and received if the ISU is unable to acquire this location, but for the ISU to receive ring alerts, the Iridium Gateway must have the current location of the ISU.

Applications where the ISU will cover large distances quickly (e.g. aircraft) and applications where the ISU will move through an environment where the ISU may not always have a good view of the sky (e.g. cities, mountainous regions) should use the Automatic SBD Network Registration capability. +SBDAREG is used to enable automatic network registration. The +SBDAREG command runs a passive geo-location algorithm which estimates the distance the ISU has moved since the previous SBD session. If the result indicates the ISU has moved 'too' far, the ISU automatically issues an updated SBD Network Registration.

Table 4-22 Automatic Registration (+SBDAREG)

Automatic Registration (+SBDAREG)	
AT+SBDAREG=1	FA sets the automatic registration to "Automatic" mode
OK	+SBDAREG response
+AREG:1,0	Unsolicited notification from +SBDAREG indicating that the registration was successful

4.7. Traffic Management

The ISU will enter traffic management mode if 2 failed SBD sessions are attempted too close together.

Traffic management prevents a transceiver from starting another SBD session for up to ten minutes. Subsequent violations will increase the delay. During the delay, +SBDIX will return error code 38. Power cycling the ISU has no effect on the traffic management period.

To check traffic management status, use +SBDLOE. This command will return two values: status, and time. Status indicates whether the time to the end of the current traffic management period could be determined - i.e. if the transceiver is connected to the network and able to acquire the current Iridium system time. Time is the amount of time until the end of the traffic management period.

Table 4-23 Possible SBDLOE Values

Possible SBDLOE Values		
Status	Time	Description
0	0	Transceiver able to acquire time and not in traffic management
0	30	Transceiver able to acquire time and in traffic management (30 seconds until end of traffic management period)
1	0	Transceiver unable to acquire time

+SBDLOE may not return immediately - it waits up to 10 seconds to acquire the Iridium system time. Examples of what the command will return while traffic management is active and inactive are shown below.

Table 4-24 +SBDLOE Example - Traffic Management Active

+SBDLOE Example - Traffic Management Active	
AT+SBDLOE	Check traffic management status
+SBDLOE:0,30 OK	30 seconds until the end of the traffic management period

Table 4-25 +SBDLOE Example - Traffic Management Inactive

+SBDLOE Example - Traffic Management Inactive	
AT+SBDLOE	Check traffic management status
+SBDLOE:0,0 OK	No traffic management period is in effect

The best way to avoid traffic management is to follow Iridium's best practices for SBD, see section 2 Best Practices for SBD Transmissions for more details.

4.8. Retrieving Transceiver Characteristics

The 9523, 9602 and 9603 transceivers have built in AT commands for identifying transceiver characteristics. These characteristics include manufacturer, model, revision information and IMEI. VARs can use these commands to fetch transceiver information on startup for logging purposes. They are also useful for troubleshooting.

4.8.1. Manufacturer Identification (+CGMI)

+CGMI can be used to fetch the transceiver's manufacturer. In the example below, the manufacturer is Iridium.

Table 4-26 Manufacturer Identification Example (+CGMI)

Manufacturer Identification Example (+CGMI)	
AT+CGMI	Query transceiver manufacturer
Iridium OK	Transceiver manufacturer (Iridium)

4.8.2. Model Identification (+CGMM)

+CGMM can be used to fetch the transceiver's model. In the example below, the model is a 9602. Both 9602 and 9603 transceivers will be listed as "IRIDIUM 9600 Family SBD Transceiver" when queried.

Table 4-27 Model Identification Example (+CGMM)

Model Identification Example (+CGMM)	
AT+CGMM	Query transceiver model
IRIDIUM 9600 Family SBD Transceiver OK	Transceiver model (9600 series)

4.8.3. Serial Number (IMEI) (+CGSN)

+CGSN can be used to fetch the transceivers serial number or IMEI.

Table 4-28 Serial Number Identification Example (+CGSN)

Serial Number (IMEI) Example (+CGSN)	
AT+CGSN	Query transceiver serial or IMEI
304050607080903 OK	Model IMEI (304050607080903)

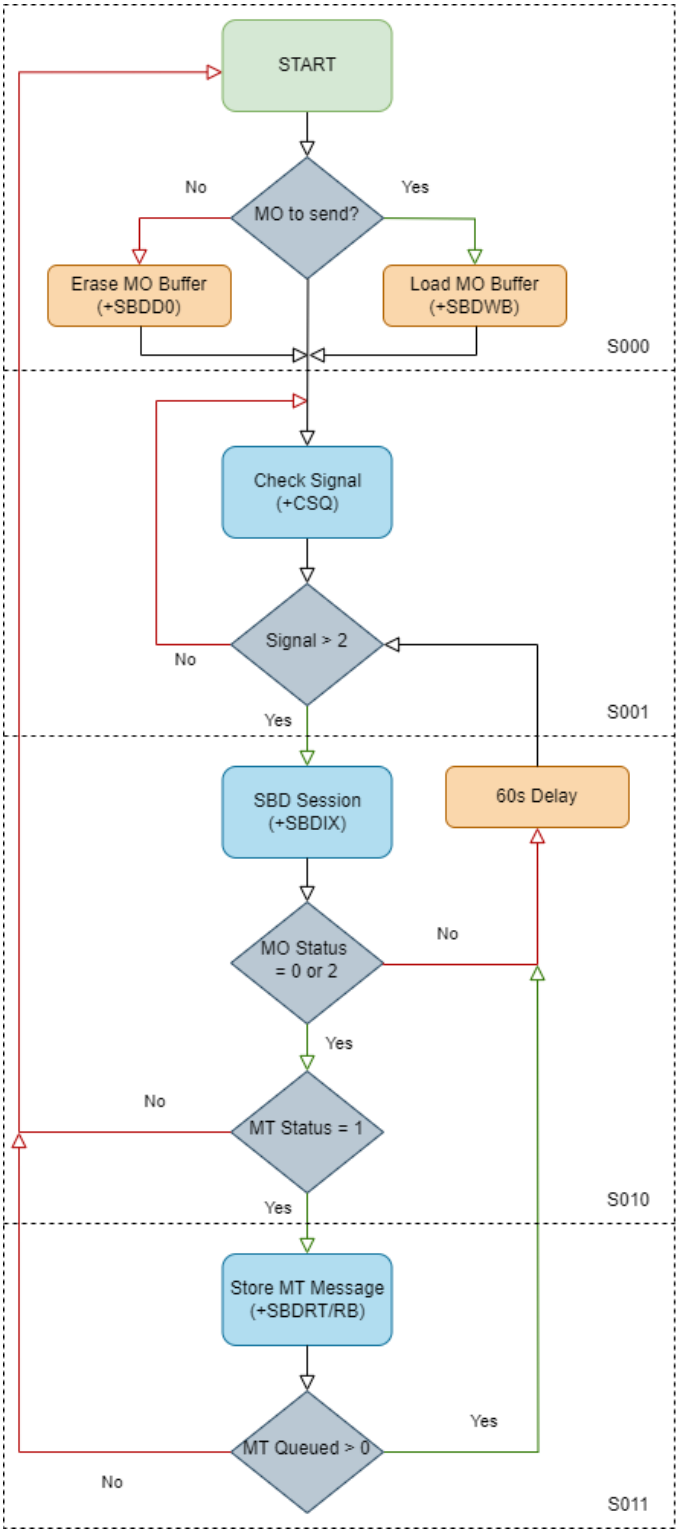
4.8.4. Revision Information (+CGMR)

+CGMR can be used to fetch revision information for the transceiver. This command will return several fields, the most important of which is the Call Processor Version or firmware version.

Table 4-29 Revision Information Example (+CGMR)

Revision Information Example (+CGMR)	
AT+CGMR	Query transceiver revision information
Call Processor Version: TA21004 Modem DSP Version: 1.7 svn: 2358 DBB Version: 0x0001 (ASIC) RFA Version: 0x0007 (SRFA2) NVM Version: KVS Hardware Version: BOOT07d4/9602NrvA-D/04/RAW0d BOOT Version: 2004 TD2-BLB960X-27 R4710 OK	Model revisions (firmware TA21004)

4.9. Sample Field Application



STATE 000 - Start

This loop can begin either in response to an SBDRING alter, for a mailbox check, or if the transceiver needs to send an MO message.

STATE 000 - Load Buffer

Prepare to start an SBD session. This state can be done in response to an SBDRING alert or if the transceiver needs to send an MO message.

- If sending a message, use +SBDWB to load the MO buffer
- If doing a mailbox check, use +SBDD0 to erase the MO buffer

STATE 001 - Check Signal

Check signal strength with +CSQ and wait until signal strength is 2 or higher.

STATE 010 - SBD Session

Start SBD session with +SBDIX.

- If MO was successfully sent (MO status 0 or 2), proceed to MT storage phase
- If the MO failed, wait 60s and retry
- If an MT message was received, store MT message

STATE 011 - Store MT

Store MT message with +SBDRT or +SBDRB.

- If there are any queued MT messages, return to start

Additional Considerations

- Developers may want to check buffer status with +SBDS
- +CIER can be used to monitor changes in signal strength but +CSQ should still be used to check signal strength immediately before an SBD session
- The MO buffer should be erased between SBD sessions to avoid duplicate messages. In this example, it's erased or overwritten before each session.

5. Direct Internet Protocol Socket "DirectIP" Interface

DirectIP is a socket-based delivery mechanism for Mobile Originated and Mobile Terminated SBD Messages and is Iridium's most popular delivery mechanism for SBD messaging. DirectIP provides lower delivery latency than the existing email protocol. It consists of a specialized socket-oriented communications protocol that utilizes direct connections between the Iridium gateway SBD subsystem and the Vendor Application. This section of the SBD Developers Guide is the DirectIP interface control document between the Iridium Gateway and the Vendor Application(s). It does not provide details of DirectIP processing within the Iridium Gateway.

The Vendor Application interface to DirectIP requires software development by the applications developer.

Iridium does not provide finished software, reference code, or applications software support for the Vendor Application. Applications developers will need to develop software to handle both Mobile Originated and Mobile Terminated DirectIP Connections. The Vendor Application should also conform to Iridium's best practices for DirectIP connections.

DirectIP is composed of separate MO and MT Iridium Gateway components. The MO DirectIP component acts as a client to the Vendor MO DirectIP server application. The MT DirectIP component acts as a server to the vendor MT DirectIP clients. In other words, the Iridium Gateway MO component seeks to establish a connection to the vendor server for MO transfers while the Iridium Gateway MT component actively listens for connections from the vendor clients for MT transfers. In either direction, clients only attach to the server when they are delivering data.

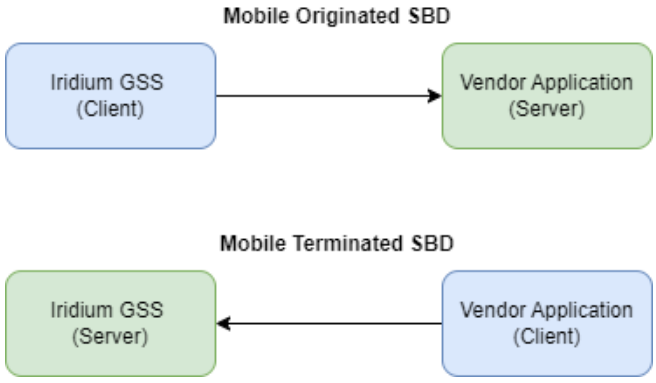


Figure 5-1 DirectIP Messaging

Both MO DirectIP and MT DirectIP protocols utilize bi-directional TCP/IP socket connections. The MO DirectIP protocol only delivers SBD MO messages from the Iridium Gateway client to the vendor server. No acknowledgement is expected from the server. In contrast, the MT DirectIP protocol delivers SBD MT messages from the vendor client to the Iridium Gateway server, and a confirmation is passed from the server back to the client indicating the success or failure of the processing of the message.

IP addresses for vendor servers must be provided to Iridium for whitelisting if VAMs wish to utilize MT messages via DirectIP. The form for whitelisting can be found at this link: https://www.iridium.com/iridium-sbd-dip-request-form/ The IP address and port for Iridium's SBD Gateway are provided on this form.

5.1. DirectIP Message Delivery

5.1.1. Mobile Originated

Upon the completion of an SBD session between the IMEI and the Iridium Gateway, the Iridium Gateway opens a socket, connects to the Vendor Application, and delivers the MO message including SBD session descriptors. Messages to the same Vendor Application are delivered in a first-in-first-out (FIFO) manner so that they are delivered in the same sequence that they are received by the Iridium Gateway. All other messages destined for the same Vendor Application are queued behind the first message while it is being delivered. Only one message is delivered per socket connection. Once a socket connection is established, a single MO message is delivered, and then the socket is closed. This sequence is repeated for every MO message queued for delivery to the vendor server. Each TCP/IP socket is only open for five seconds. If the Vendor Application doesn't transmit within that window, the connection will be automatically closed by the Iridium Gateway.

5.1.2. Mobile Terminated

When an MT message is to be queued, the Vendor Application client opens a socket, connects to the Iridium Gateway server, and delivers the MT message with disposition (see Section 5.3.5.2, "DirectIP MT Disposition Flags"). The Iridium Gateway server then parses the message, inserts the payload into the database, and sends a confirmation message back to the Vendor Application.

Once the Iridium Gateway server has inserted the payload into the database, a different process within the Iridium Gateway queues the payload for delivery and assigns an MTMSN to each. If the payload is first in the queue, it is marked as "Queued" and is ready for immediate delivery. Otherwise, it is marked as "Pending." Messages will remain in the queue for up to five (5) days. The Iridium Gateway runs a script daily (at 00:06:14) to automatically purge any messages older than five days.

5.2. Vendor Application DirectIP Server/Client Requirements

5.2.1. MT Iridium Gateway Server

- The server will listen for TCP/IP socket connections on a specific port.
- Once connected, the server will receive the entire MT message before parsing.
- The server will validate the message to ensure it meets the following criteria:
  - IMEI is of a valid format and is provisioned
  - All other input values in the MT header are valid
  - Payload length does not exceed the specified maximum
  - Iridium Gateway resources are available (the given IMEIs MT queue, overall number of active MT users)
- The server will send a confirmation message indicating the success or failure of processing the message.
- The server will terminate the socket connection once the confirmation message is sent.
- All TCP/IP connections are closed by the Gateway after 5 seconds.
- If the connection fails at any point prior to sending the confirmation message, the MT message will be dropped.

5.2.2. MT Vendor Client

- The client will seek to establish a TCP/IP socket connection to the IP address of the Iridium Gateway MT DirectIP server on a specified port.
- Once connected, the client will transmit the MT payload and wait for the confirmation message.
- Once the confirmation message has been transmitted / received, the client will allow the server to close the socket connection.

5.2.3. MO Iridium Gateway Client

- The client will seek to establish a TCP/IP socket connection to the IP address and port provisioned for the originating IMEI.
- Once connected, the client will transmit the MO payload and close the socket connection.
- If no connection is established, the client will implement the retry scheme outlined in the following section.
- Once the message has been transmitted, the client will close the socket connection. No acknowledgement from the server will be expected.

5.2.4. MO Vendor Server

- The server will listen for TCP/IP socket connections on a specific port. This specific port should be specified during provisioning.
- Once connected, the server will receive the entire MO message before parsing.
- The server will allow the Iridium Gateway client to close the socket connection.
  - Client Side (DMO process at IST)
    - Open connection (a socket connection)
    - Send data over socket
    - Close connection (close the socket)
  - Server Side (Customer App)
    - Accept Connection
    - Read header body
    - Close socket. (This action allows the socket to be returned into available use) A common TCP/IP 'best practice' is to close the socket connection from both sides.
- Five delivery destinations are provided for each Iridium transceiver. One of these destinations should be used as a backup destination should the primary vendor server fail. This will prevent the MO queue at the Iridium Gateway from backing up (see following section).

5.2.5. Vendor Application Server Unavailable

If the initial attempt to connect to the vendor application times out, the subsequent MO message delivery will not take place and subsequent connection attempts will be made. A retry scheme has been implemented to back off delivery attempts to unreachable servers. Retries will occur after 1, 5, 10, 20, 30, 60, 120, 240, and 360 seconds with the maximum of 360 seconds used for every retry thereafter. Connection attempts continue to be made for up to 12 hours. Each individual message has a lifetime of 12 hours starting at the time that the payload was received at the Iridium Gateway. If it can’t be delivered within this timeframe, it will be marked as "DirectIP_Timeout" in the SBD database and removed from the delivery queue.

Up to 10,000 messages may be queued for a specific Vendor Application. If this limit is exceeded, payloads will be deleted from the front of the queue (the "oldest" payloads.)

5.3. DirectIP Overall Message Structure

The overall message structure for both MO and MT DirectIP is shown in Table 5-1. When a connection is first established, the receiving application will receive three bytes. The first is a general DirectIP protocol revision number (this document describes revision 1). The following two bytes indicate the number of bytes that make up the body of the message that is made up of some number of information elements. This enables the receiving end to know deterministically when all bytes transferred have been received. This value must be accurate for the Gateway to transmit/receive and process the message. Otherwise, the message will fail.

Table 5-1 DirectIP Overall Message Format

DirectIP Overall Message Format			
Field Name	**Data Type**	**Length (Bytes)**	**Range of Values**
Protocol Revision Number	char	1	1
Overall Message Length	unsigned short	2	N
Message Information Elements	variable	N	N/A

5.3.1. Information Elements

To maintain maximum flexibility within the protocol, all data to be transferred has been segmented into information elements (IEs). Information elements (IEs) consist of a 1-byte IE ID, 2-byte IE length and IE contents. Those IEs currently defined are shown in detail in Section 5.3.4, “Mobile Originated Message Formatting” and Section 5.3.5, “Mobile Terminated Message Formatting”. The general format of each IE is the same and is shown in Table 5-2.

Table 5-2 DirectIP Information Element General Format

DirectIP Information Element General Format		
Field Name	**Data Type**	**Length (bytes)**
Information Element ID (IEI)	char	1
Information Element Length	unsigned short	2
Information Element Contents	variable	N

5.3.1.1. Parsing Information Elements

Vendor applications should parse IEs by reading the first byte, then reading the IE length and using that length to iterate through the remaining bytes. Then the application will proceed to the next IE and step through that IE accordingly. For MT messages sent to the gateway, it is essential that all required IEs and IE lengths be present in the message. If there are too many or too few bytes received as determined by the Gateway’s parser, the message will be dropped, and an error will be returned to the VA in the confirmation message. Available Information Elements can be found in the following table.

Table 5-3 Available DirectIP Information Elements

Available DirectIP Information Elements	
Information Element	IEI Value
MO Header IEI	0x01
MO Payload IEI	0x02

Available DirectIP Information Elements	
MO Location Info IEI	0x03
MO Confirmation IEI	0x05
MT Header IEI	0x41
MT Payload IEI	0x42
MT Confirmation Message IEI	0x44
MT Message Priority IEI	0x46

5.3.2. Byte Alignment

The entire message transfer will be treated as a byte stream. This enables the various data types contained within the message to be transferred with no consideration given to the byte alignment of the data types and for the compacting of the fields to the appropriate sizes. Multi-byte fields are transmitted in network byte order (big endian). For example, the four-byte field 0x0a0b0c0d is transmitted as in the following table.

Table 5-4 DirectIP Byte Alignment Example

DirectIP Byte Alignment Example				
Byte address	0	1	2	3
Bit offset	01234567	01234567	01234567	01234567
Binary	00001010	00001011	00001100	00001101
Hex	0a	0b	0c	0d

5.3.3. Message Sequence Numbers

The MOMSN and MTMSN are unique to each ISU and correspond to the number of MO and MT messages transmitted by the ISU. Because these sequence numbers are stored locally in a register on the ISU itself, they will roll over at 65535. Due to the bidirectional nature of SBD transmissions, both the MOMSN and MTMSN are included in every message. If an MT payload transfer was attempted, the MTMSN will be included in the header regardless of the success of the session. If the session failed, the payload is still queued for delivery. If no MT delivery attempt was made in the session, this value will be zero.

5.3.4. Mobile Originated Message Formatting

5.3.4.1. MO DirectIP Header

The information in this header is required as part of every DirectIP MO message delivery. It includes all the information necessary to uniquely identify the SBD MO message. It also includes the overall SBD session status and identifier (MTMSN) for the associated MT message delivery, if any.

Table 5-5 DirectIP MO Header Information Element

DirectIP MO Header Information Element			
Field Name	**Data Type**	**Length (bytes)**	**Value(s)**
MO Header IEI	char	1	0x01 (hex)
MO header IE ID, fixed field			
MO Header Length	unsigned short	2	28 (decimal)
Length of the MO header, fixed field			
CDR Reference (Auto ID)	unsigned integer	4	Between 0 - 4294967295 (decimal)
Unique identifier used to differentiate call data records (CDRs) in the Iridium Gateway Database			
IMEI	char	15	ASCII Numeric Characters
15-digit identifier unique to each Iridium device			
Session Status	unsigned char	1	0-15 (decimal)
Indicates message success/failure and any errors present			
MOMSN	unsigned short	2	1 - 65535 (decimal)
Mobile Originated Message Sequence Number (MOMSN) associated with the SBD session, set and incremented by the ISU before being transmitted to the Gateway			
MTMSN	unsigned short	2	0 - 65535 (decimal)
Mobile Terminated Message Sequence Number (MTMSN) associated with the SBD session, set by the Iridium Gateway and before the MT message is queued for delivery			
Time of Session	unsigned integer	4	Epoch Time
UNIX epoch time in UTC			

5.3.4.2. MO Session Status

This field provides an indication of success of the SBD session between the IMEI and the Iridium Gateway associated with the over-the-air payload delivery. If the message delivery was unsuccessful, no payload will be included in the MO message. This value is independent of the MT session status and only indicates success or failure of the MO portion of the corresponding SBD session.

Table 5-6 MO Session Status

MO Session Status	
Value	**Description**
0	The SBD session completed successfully.
1	The MO message transfer, if any, was successful. The MT message queued at the Iridium Gateway is too large to be transferred within a single SBD session.
2	The MO message transfer, if any, was successful. The reported location was determined to be of unacceptable quality. This value is only applicable to IMEIs using SBD protocol revision 1.
10	The SBD session timed out before session completion.
12	The MO message being transferred by the IMEI is too large to be transferred within a single SBD session.
13	An RF link loss occurred during the SBD session.
14	An IMEI protocol anomaly occurred during SBD session.
15	The IMEI is prohibited from accessing the Iridium Gateway.

5.3.4.3. Time of Session

This field provides a UTC timestamp of the IMEI session between the IMEI and the Iridium Gateway in the format of an epoch time integer. The epoch time is the number of seconds since the start of the UNIX epoch at 1/1/1970 00:00:00.

Format: epoch time integer

Resolution: 1 second

5.3.4.4. MO Payload

The MO header is followed by the MO payload. This information element includes the actual MO payload delivered from the IMEI to the Iridium Gateway during the SBD session identified in the header. In an MO message delivery related to a mailbox check session (empty payload) or a failed session, no payload will be included.

Table 5-7 MO Payload IEI

MO Payload IEI			
Field Name	**Data Type**	**Length (bytes)**	**Value(s)**
MO Payload IEI	char	1	0x02 (hex)
MO payload IE ID, fixed field			
MO Payload Length	unsigned short	2	0 - 1960 (decimal)
Length of the MO payload			
MO Payload	char	1 - 1960	Payload bytes in hex
Actual MO payload sent from the ISU to the Gateway			

5.3.4.5. MO Location Information

Location information for the ISU can be optionally included in MO messages via SPNet. If enabled, this information will be appended to the MO header after the time of session field. The CEP radius provides the radius around the center point within which the unit is located. While the resolution of the reported position is given to 1/1000th of a minute, it is only accurate to within 10Km 80% of the time. If precise location values are needed, Iridium recommends using a separate GPS antenna or other external GPS device.

Table 5-8 MO Location Information IE

MO Location Information IE			
Field Name	Data Type	Length (bytes)	Value(s)
MO Location Information IEI	char	1	0x03 (hex)
MO location information IE ID, fixed field			
MO Location Information Length	unsigned short	2	20 (decimal)
Length of the MO location information IE, fixed field			
Latitude/Longitude	Double	7	Variable
The latitude and longitude provide a center point of the estimated location and are derived from the LGC coordinates output from the CPLD exchange during the SBD session.			
CEP Radius	unsigned integer	4	1 - 2000 (decimal)
The CEP radius provides the radius (in Kilometers) around the center point within which the IMEI is located with an 80% probability of accuracy.			

Formatting for the lat/long information is described in Table 5-9.

Table 5-9 MO Location Data Format

Location Data Format			
Field		Byte Number	Description & Allowed Values
Bits 0-3*	Reserved	1	0
Bits 4-5	Format Code		0
Bit 6	NSI		NSI: North/South Indicator (0=North, 1=South)
Bit 7	EWI		EWI: East/West Indicator (0=East, 1=West)
Latitude (degrees)		2	Decimal Range: 0 to 90 Hex Range: 0x00 to 0x5A
Latitude (thousandths of a minute, MS-Byte)		3	Decimal Range: 0 to 59,999 (unsigned integer, American notation) Hex Range: 0x0000 to 0xEA5F
Latitude (thousandths of a minute, LS-Byte)		4	
Longitude (degrees)		5	Decimal Range: 0 to 180 Hex Range: 0x00 to 0xB4
Longitude (thousandths of a minute, MS-Byte)		6	Decimal Range: 0 to 59,999 (unsigned integer, American notation) Hex Range: 0x0000 to 0xEA5F
Longitude (thousandths of a minute, LS-Byte)		7	

NOTE In byte 1, MSB or bit 0 is the left most bit. I.e. if byte 1 is 1010 0000, then the first digit (1) would be bit 0.

5.3.4.6. Successful MO Message Delivery Example

Table 5-10 gives an example of a byte stream for a typical MO DirectIP message following a successful SBD session. Note that the IMEI has been provisioned such that the geolocation information is not included in the message.

Table 5-10 Successful MO Message Delivery Example

Successful MO Message Delivery Example			
Field Name	**Length (bytes)**	**Hex**	**Value**
Protocol Revision Number	1	01	1
Overall Message Length	2	00 29	48
MO Header IEI	1	01	1
MO Header Length	2	00 1C	28
CDR Reference	4	00 12 D6 87	1234567
IMEI	15	33 30 30 30 33 34 30 31 30 31 32 33 34 35 30	300034010123450 (ASCII)
Session Status	1	00	0 (Transfer OK)
MOMSN	2	D4 31	54,321
MTMSN	2	30 39	12,345
Time of Session	4	67 0E 6E BB	1728999099 (10/15/24 13:31:39)
MO Payload IEI	1	02	2
MO Payload Length	2	00 07	7
MO Payload	7	74 65 73 74 31 32 33	test123 (ASCII)

5.3.4.7. Failed MO Message Delivery Example

Table 5-11 gives an example of a byte stream for an MO DirectIP message following a failed SBD session due to an incomplete transfer. Note that no payload is included.

Table 5-11 DirectIP MO Message Delivery Example - Failed SBD Session

DirectIP MO Message Delivery Example - Failed SBD Session			
Field Name	**Length (bytes)**	**Hex**	**Value**
Protocol Revision Number	1	01	1
Overall Message Length	2	00 1F	31
MO Header IEI	1	01	1
MO Header Length	2	00 1C	28
CDR Reference	4	00 13 DC 3F	1301567
IMEI	15	33 30 30 30 33 34 30 31 30 31 32 33 34 35 30	300034010123450 (ASCII)
Session Status	1	0D	13 (Incomplete Transfer)
MOMSN	2	D4 32	54322
MTMSN	2	00 00	0
Time of Session	4	67 0E 6E BB	1728999099 (10/15/24 13:31:39)

5.3.5. Mobile Terminated Message Formatting

5.3.5.1. MT DirectIP Header

The information in this header is required as part of every DirectIP MT message delivery. All portions of this header must be present and correct for the message to be successfully queued at the Gateway. An example of a successful MT message delivery, including confirmation message, can be found in Section 5.3.5.5, “DirectIP MT Message Delivery Example”.

Table 5-12 DirectIP MT Header IE

DirectIP MT Header IE			
Field Name	**Data Type**	**Length (bytes)**	**Value(s)**
MT Header IEI	char	1	41 (hex)
MT header IE ID, fixed field			
MT Header Length	unsigned short	2	28 (decimal)
Length of the MT header, fixed field			
Unique Client Message ID	unsigned integer	4	From client (not MTMSN)
Message ID chosen by vendor application, used for identification purposes for VA			
IMEI	char	15	ASCII Numeric Characters
15-digit identifier unique to each Iridium device			
MT Disposition Flags	unsigned char	2	See 5.3.5.2 DirectIP MT Disposition Flags
Govern functions such as flush MT queue, message priority and sending additional ring alerts			

5.3.5.2. DirectIP MT Disposition Flags

The MT disposition flags govern additional features related to MT deliveries such as message priority, flush MT queue, and sending an additional ring alert to a device. These features are only available via DirectIP. The MT disposition flags are contained in a 2 byte bit map with 16 available flags. Available flags and corresponding values are shown in the table below.

Table 5-13 MT Disposition Flags

DirectIP MT Disposition Flags			
Disposition Flag	**Value (decimal)**	**Value (hex)**	**Description**
Flush MT Queue	1	00 01	Delete all MT payloads in the SSD's MT queue
Send Ring Alert (no payload)	2	00 02	Send ring alert with no associated MT payload (normal ring alert rules apply)
High Priority Message	16	00 10	Place the associated MT payload in queue based on priority level
Assign MTMSN	32	00 20	Use the value in the Unique ID field as the MTMSN

Combining Disposition Flags

Disposition flags may be combined to trigger multiple actions within a single MT message delivery. However, there are only two available combinations: Flush MT Queue/Send Ring Alert (no payload) and Flush MT Queue/Assign MTMSN. Send Ring Alert and Assign MTMSN flags must not both be set because Send Ring Alert requires that there be no MT payload, and Assign MTMSN requires that there be an MT payload. If the Assign MTMSN flag is present then Include Payload IE must also be present, otherwise the message will return a protocol error.

Flush MT Queue

When this flag is set, all payloads in the MT queue for the given IMEI are deleted. If a payload is included in the MT message, it will be queued after the currently queued payloads, if any, have been deleted. This enables the Vendor Application to maintain a queue depth of one, overwriting any previous payload queued.

Send SBD Ring Alert - No MT Payload

When this flag is set, the Iridium Gateway sends an SBD Ring Alert to the specified IMEI even though no new MT message is being queued. To receive this additional ring alert, the ISU must have ring alerts enabled and the Iridium network must have the ISU's updated location information. If successful, two ring alerts will be sent to the device (20 seconds apart), i.e. normal ring alert rules apply. For this flag to work, there must be no MT payload present in the message.

NOTE

Excessive use of this feature could result in restrictions being imposed on the offending IMEIs. This feature should not be used to compensate for poor FA design or situations where the IMEI may be frequently powered off. In such cases, Mailbox Checks should be used to check for queued MT messages.

High Priority Message

MT message prioritization allows the vendor to set the priority of the incoming MT payload relative to the other MT payloads already queued for the associated SSD. When this flag is set, the delivered payload will be placed in MT queue for the given SSD based on a priority level included in a separate information element.

Table 5-14 MT Priority IE

MT Priority IE		
Field Name	**Length (Bytes)**	**Value(s)**
MT Priority IEI	1	0x46 (hex)
MT Priority Length	2	2 (decimal)
Priority Level	2	1-5 (decimal)

There are five priority levels, where 1 is the highest priority and 5 is the lowest priority. Payloads without a specified priority level will automatically be assigned lowest priority (P5). Payloads with a priority specified will be placed in front of payloads with lower priority but not in front of payloads with equal or higher priority. Payloads of equal priority will be treated in a first-in-first-out (FIFO) manner. When another MT message is to be queued for delivery over the air, the GSS selects the oldest message with the highest priority. If the MT queue for the SSD is full, the handling of the payload depends on the priority level of the new payload and that of the payloads in the queue. If the new payload is lower priority than all other payloads in the queue, it will be rejected. Otherwise, the oldest payload (i.e. first in the FIFO) of the lowest priority present in the queue will be deleted, even if the lowest priority matches the new priority received. For example, if the queue is full with all payloads assigned P1, a new P1 payload will bump the oldest P1 payload from the queue.

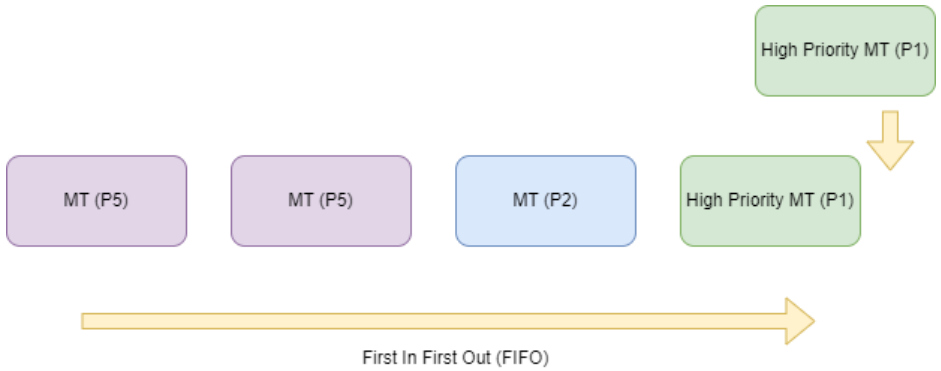


Figure 5-2 MT Queue Priority

NOTE

If prioritization is utilized, the MTMSN of payloads transmitted to the SSD may no longer be in numeric sequential order. The MTMSN is assigned at the time that the payload is added to the MT queue and not when it is transmitted to the SSD. If a payload is received that is placed in front of lower priority payloads in the queue, it will have a higher MTMSN that the lower priority payloads that are delivered afterwards.

Assign MTMSN

When this flag is set, the GSS will use the value in the Unique Client ID field in the message header as the MTMSN for the associated MT message payload. Because the MTMSN is a 16-bit field, the Unique ID (a 32-bit field) must be between 1 to 65,535. Any value not in this range will cause the MT delivery to fail with an MTMSN out-of-range error.

The MTMSN normally used is an internally maintained value for each IMEI independent of all other IMEIs. When the assign MTMSN flag is not used, the GSS will use this value for the given IMEI incremented by one. When this flag is used, the assigned MTMSN only affects the associated MT message. The internally tracked value remains unchanged and will be used for all subsequent messages when the flag is not set.

5.3.5.3. MT Payload

This information element includes the actual MT payload to be queued and delivered over the air to the destination IMEI. Inclusion of this IE in the MT delivery is optional based on the disposition flags included in the header (see previous section 6.3.5.2 DirectIP MT Disposition Flags.)

Table 5-15 MT Payload IE

MT Payload IE			
Field Name	**Data Type**	**Length (bytes)**	**Value(s)**
MT Payload IEI	char	1	0x02 (hex)
MT payload IE ID, fixed field			
MT Payload Length	unsigned short	2	1 - 1890 (decimal)
Length of the MT payload			
MT Payload	char	1 - 1890	Payload bytes in hex
Actual MT payload sent from the VA to the Gateway			

5.3.5.4. DirectIP MT Message Confirmation Message

A confirmation message indicating the status of the processing of the MT message is sent to the vendor client from the Iridium Gateway for every MT message received.

Table 5-16 DirectIP MT Confirmation Message

DirectIP MT Confirmation Message			
Field Name	**Data Type**	**Length (bytes)**	**Value(s)**
MT Confirmation Message IEI	char	1	0x44 (hex)
MT confirmation message IE ID, fixed field			
MT Confirmation Msg Length	unsigned short	2	25 (decimal)
Length of the MT confirmation message			
Unique Client Message ID	integer	4	From Client (not MTMSN)
Message ID chosen by vendor application, used for identification purposes for VA			
IMEI (User ID)	char	15	ASCII Numeric Characters
15-digit identifier unique to each Iridium device			
Auto ID Reference	unsigned integer	4	0 - 4294967295 (decimal)
Unique identifier used to differentiate call data records (CDRs) in the Iridium Gateway Database			
MT Message Status	short	2	Order of message in IMEI's queue or error reference
Indicates success or failure of MT message and any errors present			

NOTE In Iridium Web Services (IWS) call data records, the Auto ID Reference may sometimes contain leading bytes. MT Confirmation messages received directly via DirectIP automatically strips out these leading bytes.

MT Message Status

Every MT confirmation message returns a status value indicating that the overall MT message was received and validated and that the payload was queued successfully or that a failure occurred. If successful, the value is a positive number indicating the order of the received payload in the IMEI's associated MT message queue. If not successful, the value will be a negative number serving as an error code specifying the problem detected. Table 5-17 shows the possible status values including the error codes.

Table 5-17 MT Message Status Codes

MT Message Status Codes	
Status	Description
1 - 50	Successful, order of message in the MT message queue
0	Successful, no payload in message
-1	Invalid IMEI - too few characters, non-numeric characters
-2	Unknown IMEI - not provisioned on the Iridium Gateway
-3	Payload size exceeded maximum allowed (See Section 1.0)
-4	Payload expected, but none received
-5	MT message queue full (max of 50)
-6	MT resources unavailable
-7	Violation of MT DirectIP protocol error
-8	Ring alerts to the given IMEI are disabled
-9	The given IMEI is not attached (not set to receive ring alerts)
-10	Source IP address rejected by MT filter
-11	MTMSN value is out of range (valid range is 1 - 65,535)

NOTE The last two error values (-8 and -9) only apply when the "Send Ring Alert" disposition flag has been set.

5.3.5.5. DirectIP MT Message Delivery Example

Table 5-18 gives a successful DirectIP MT delivery example.

Table 5-18 Successful DirectIP MT Message Example

Field Name	Length (bytes)	Hex	Value (in ASCII, if applicable)
DirectIP MT Header			
Protocol Revision Number	1	01	1
Overall Message Length	2	00 22	34
MT Header IEI	1	41	65
MT Header Length	2	00 15	21
Unique Client Message ID	4	6D 73 67 32	msg1 (ASCII)
IMEI (Device ID)	15	33 30 34 30 35 30 36 30 37 30 38 30 39 30 33	304050607080903 (ASCII)
MT Disposition Flags	2	00 00	0
MT DirectIP Payload			
MT Payload IEI	1	42	66
MT Payload Length	2	00 07	7
MT Payload	7	74 65 73 74 31 32 33	test123 (ASCII)

Table 5-19 provides an example for the corresponding confirmation message returned from the Iridium Gateway.

Table 5-19 Successful DirectIP MT Confirmation Example

Field Name	Length (bytes)	Hex	Value (in ASCII, if applicable)
Protocol Revision Number	1	01	1
Overall Message Length	2	00 1C	28
MT Confirmation Message IEI	1	44	68
MT Confirmation Message Length	2	00 19	25
Unique Client Message ID	4	6D 73 67 31	msg1 (ASCII)
IMEI (Device ID)	15	33 30 34 30 35 30 36 30 37 30 38 30 39 30 33	304050607080903 (ASCII)
Auto ID Reference	4	48 85 22 D7	1216684759
MT Message Status	2	00 03	3rd position in queue at gateway

6. Email Description

For ISU's provision to use email, each MO or MT message the VA will receive an email for each session that reaches the Iridium Gateway regardless of any message transfer, unless one or both ISUs are provisioned to send to another ISU, in which case only the ISU provisioned to send to an email address will receive email notifications. This section describes in more detail the operation of Mobile Terminated and Mobile Originated email delivery service. 'ISU to ISU' mode, which is independent of email or IP Socket, is described separately in Section 5 Direct Internet Protocol Socket "DirectIP" Interface.

Email delivery is intended for testing purposes only. Either DirectIP or Iridium Cloud Connect SBD should be used for production solutions.

NOTE GSS email interface is not available for SBD traffic through the gateway in Izhevsk, Russia (Ижéвск).

6.1. Email MO

Mobile Originated (MO) messages function the same way as DirectIP MO messages, except the receiving destination will be an email address instead of an IP and port. MO messages are sent to the Iridium Gateway from the ISU and then distributed by the Gateway's email service to the specified destination email address.

The actual MO payload will be carried as a binary attachment to an email from the Iridium Gateway to the destination email address. The binary attachment is encoded using standard MIME Base64 encoding as defined in RFC 2045. This attachment will be in a .sbd file which can be read into a VA programmatically or viewed in any standard text editor. If the original MO message wasn't in ASCII, it won't display in human-readable characters in a text editor and must first be converted to hex.

Unlike Mobile Terminated messages sent to the Iridium Gateway, Mobile Originated messages sent to the Vendor Application carry additional information in the email message body. This information includes the Mobile Originated Message Sequence Number (MOMSN), the time of the session, the session status, the message size, and optional ISU specific geo-location information. The format of such an email message is provided in Table 6-1, details of the email message fields are provided in Table 6-3.

NOTE The ISU location information can be excluded from MO messages by un-checking "Include Geo Data" on SPNet when provisioning the ISU. An example of an email message with no geo-location information is shown in Table 6-2.

Table 6-1 Email MO with Location Information

Email MO with Location Information	
Header	From: sbdservice@sbd.iridium.com Sent: Tuesday, August 13, 2024 12:49 PM Subject: SBD Msg From Unit: 304050607080903
Body	MOMSN: 23 MTMSN: 0 Time of Session (UTC): Tue Aug 13 16:51:04 2024 Session Status: 00 - TRANSFER OK Message Size (bytes): 351 Unit Location: Lat = 59.372463 Long = 75.309806 CEPradius = 3 Message is Attached.
Attachment	.sbd file containing binary encoded message bytes

Table 6-2 Email MO without Location Information

Email MO without Location Information	
Header	From: sbdservice@sbd.iridium.com Sent: Friday, July 8, 2024 00:12 AM Subject: SBD Msg From Unit: 300003000210150
Body	MOMSN: 652 MTMSN: 644 Time of Session (UTC): Fri Jul 8 00:12:55 2024
Attachment	.sbd file containing binary encoded message bytes

6.1.1. Mailbox Checks

The Iridium Gateway will send a confirmation email when an ISU performs a mailbox check. This email will be identical to a standard email MO message but will have no attached MO message.

6.1.2. Overview of Email MO Fields

These fields are identical to fields used for DirectIP MO.

Table 6-3 DirectIP MO Fields

DirectIP MO Fields	
Field Name	**Description**
From	Identifies the sender of the SBD service, should be sbdservice@sbd.iridium.com
Sent	Time when the message was sent from the Iridium Gateway to the destination email address in UTC
Subject	IMEI of the unit sending the MO message
MOMSN	Mobile Originated Message Sequence Number
MTMSN	Mobile Terminated Message Sequence Number
Time of Session	UTC timestamp of the ISU session between the ISU and the Iridium Gateway in the following format: "DDD MMM dd HH:MM:SS yyyy"
Session Status	MO message status, identical to MO status included for MO DirectIP
Message Size	Message size in bytes of the attached message
Unit Location	Lat/long coordinates and CEP radius for the ISU sending the MO message

6.2. Email MT

Mobile Terminated (MT) messages sent via email function similarly to MT messages sent via DirectIP, except that MT formatting is largely handled by the Gateway's email service. When sending MT messages to an ISU via email, standard MT requirements apply:

- The ISU must be provided in SPNet to send Ring Alerts.
- The MT message must not exceed the maximum allowed MT message size for the given ISU

To send an MT message via email:

- Add data@sbd.iridium.com as the recipient
- Put the IMEI of the transceiver in the subject line
  - Email MTs can be sent to up to 4 ISUs at once; multiple ISUs should be separated by spaces in the subject line
- Ensure that the body of the message is empty
- Attach a .sbd file containing the MT message to the email. Ex: 'testdata.sbd'
  - File names must be 80 characters or less and are not case sensitive.
  - Files should use Base64 encoding and use the .sbd extension. If files have an incorrect extension (something other than .sbd) an error indication email will be sent to the email address attempting to send the message.
  - Multiple messages can be queued for delivery to the specified ISUs by including multiple attachments
- Send the message

Table 6-4 Email MT Message Example

Email MT Message Example	
TO:	data@sbd.idirium.com
FROM:	developer@domain.com
SUBJECT:	304050607080903
BODY:	EMPTY
ATTACHMENT:	.sbd file containing MT message

6.2.1. Email MT Queued at Gateway Confirmation

If an MT message sent via email has been successfully queued at the Gateway, a confirmation message will be returned to the sending email address. Similarly, if the message could not be queued, an error message will be returned.

Table 6-5 Email MT Queued at Gateway Confirmation Example

Email MT Queued at Gateway Confirmation Example	
TO:	developer@domain.com
FROM:	sbdservice@sbd.iridium.com
SUBJECT:	SBD Mobile Terminated Message Queued for Unit: 304050607080903
BODY:	The following mobile-terminated message was queued for delivery: IMEI: 304050607080903 Time: Fri May 26 15:24:22 2024 Attachment Filename: testdata_518.sbd Attachment Size: 518 The MTMSN is 6870, and the message is number 2 in the queue.

Table 6-6 Email MT Not Queued at Gateway Confirmation Example

Email MT Not Queued at Gateway Confirmation Example	
TO:	developer@domain.com
FROM:	sbdservice@sbd.iridium.com
SUBJECT:	Subject: Error: SBD Mobile-Terminated Message Not Queued for Unit: 300001001247240
BODY:	The following mobile-terminated message was not queued for delivery: IMEI: 304050607080903 Time: Mon Oct 27 17:23:30 2024 Attachment Filename: testdata_518.sbd Attachment Size: 518 bytes Reason: Mobile-termination message queue for the IMEI is full (max of 50 allowed).

6.2.2. Overview of Email MT Confirmation Message Fields

Table 6-7 Email MT Confirmation Message Fields

Email MT Confirmation Message Fields	
Field Name	Description
To	Sender of the email MT
From	Identifies the sender of the SBD service, should be sbdservice@sbd.iridium.com
Subject	IMEI of the unit sending the MO message and confirmation that the MT message has been queued and/or error code if the MT could not be queued
Time	UTC timestamp of the ISU session between the ISU and the Iridium Gateway in the following format: "DDD MMM dd HH:MM:SS yyyy"
IMEI	IMEI for the ISU for which the MT message was queued
Attachment Filename	Filename for the attachment containing the MT message
Attachment Size	Message size in bytes of the MT message in the attachment
MTMSN	Mobile Terminated Message Sequence Number
Queue Position	If successfully queued, the position in the queue where the MT was placed
Reason	Error code if message could not be queued

Table 6-8 Possible Error Codes for Email MT Messages

Possible Error Codes for Email MT Messages
Reason: IMEI length (M) is invalid - must be 15 characters.
Reason: The IMEI (300xxxxxxxxxxx) is not provisioned on the SBD system.
Reason: No attachment with a '.sbd' file extension was found
Reason: Payload size is too large (max size allowed is XXXX bytes).
Reason: Mobile-termination message queue for the IMEI is full (max of 50 allowed).

6.2.3. MT Retrieved by ISU Confirmation

The Iridium Gateway will send an additional confirmation message via email when an MT has been successfully picked up by the ISU. This confirmation message will be sent to destination email addresses regardless of if the original MT was queued via email or DirectIP.

Table 6-9 MT Retrieved by ISU Confirmation Example

MT Retrieved by ISU Confirmation Example	
FROM:	sbdservice@sbd.iridium.com
TO:	developer@domain.com
BODY:	MOMSN: 7335 MTMSN: 0 Time of Session (UTC): Sat Sep 14 19:46:09 2024 Session Status: 00 - Transfer OK Message Size (bytes): 0

NOTE MT disposition flags are not available via email.

7. ISU-ISU Messages

Messages from ISU #1 are to a second ISU (ISU #2) without leaving the Iridium network. [See Figure 7-1.] This option requires provisioning by the Value Added Reseller through SPNet. ISU #1 can be provisioned to send the same MO-SBD message to up to five ISUs. Note that there is an ability to deliver a MO-SBD message to up to 5 DirectIp delivery destinations. It is also possible to mix and match email, ISU, SSD-SSD and direct IP destinations for MO-SBD messages.

ISU-ISU SBD messages are billed twice. Once as a MO-SBD message to the initiating ISU IMEI and once as a MT-SBD message to the terminating ISU IMEI.

The MO-SBD message from ISU #1 is placed into the MT-SBD queue of ISU #2 when it has been received by the Iridium Gateway. The MO-SBD message is never delivered to the Vendor Application as no email address can be programmed for the Vendor Application. No SBD session descriptors are delivered to either the originating or terminating ISU. However, if ISU #2 is provided to send MO-SBD messages to a VA, then the mailbox check or sending of a MO-SBD message will cause an email message indicating the mailbox check or the transmission of the MO-SBD message to the Vendor Application. There are five error conditions that can occur in ISU-ISU SBD messaging as shown below.

Table 7-1 Possible ISU-ISU Errors

Possible ISU-ISU Errors	
Error Condition	**Action**
Message size = 0 bytes	MT-SBD message will not be queued and will be deleted
Message Size > 270 bytes when ISU #2 is a 9601 or 9602 SBD Transceiver	MT-SBD message will not be queued and will be deleted
Message size > 1890 bytes when ISU #2 is a 9522, 9522A or 9522B LBT	MT-SBD message will not be queued and will be deleted
Destination ISU MT queue > 50 messages	If the destination ISU MT queue is full the MT-SBD message will not be queued
Destination ISU is not provisioned	If the destination ISU is not provisioned the MT-SBD message will not be queued

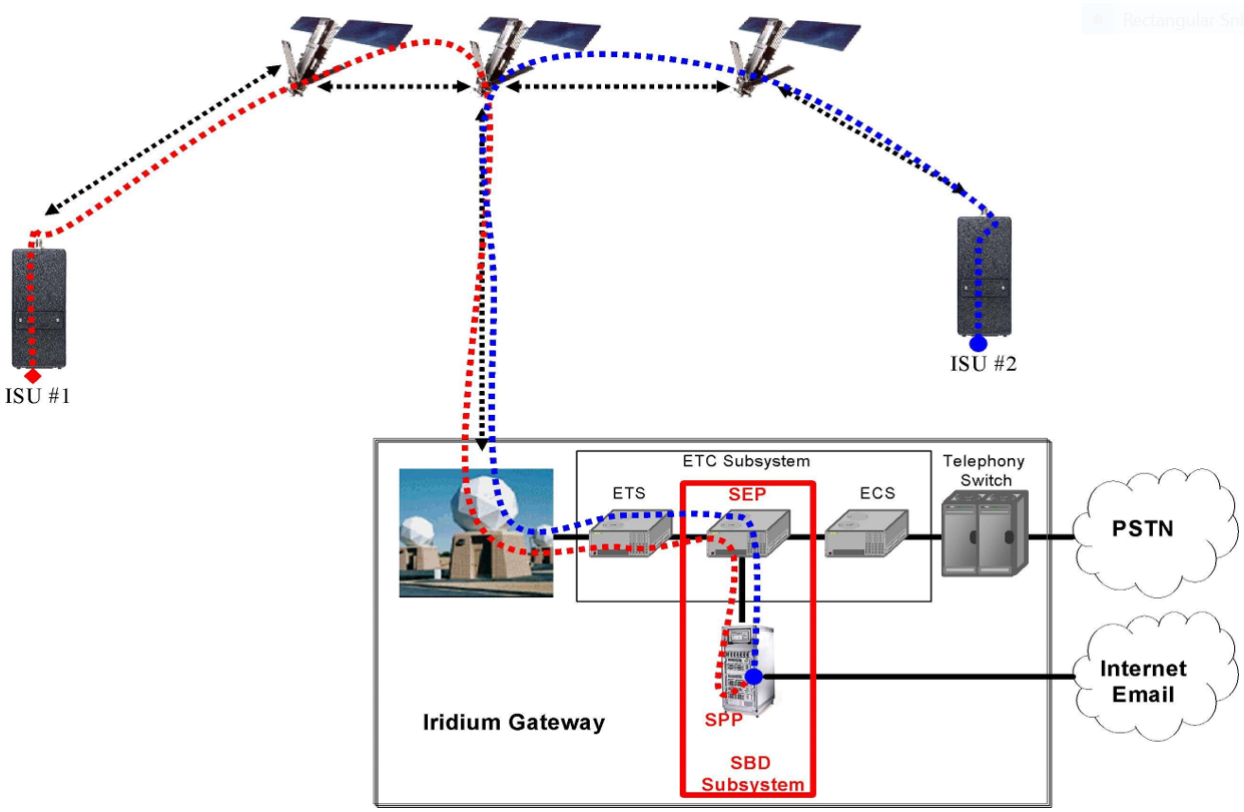


Figure 7-1 SBD Call Routing for ISU-ISU Messages

8. Iridium Short Burst Data Service Security Features

The Iridium System supports the GSM-specified algorithm A3 for authentication security, but not algorithms A5/A8 for channel encryption. Table 8-1 summarizes the security features explicitly designed into the Iridium system.

NOTE A3 is only used in transceivers using a SIM card.

Table 8-1 Baseline Iridium Security Features

Baseline Iridium Security Features	
Authentication	**A3 (128-bit Key)**
Equipment Anti-Theft Validation	Global Equipment Identity Register
Anonymity (User location confidentiality)	TMSI based
Signaling Message Confidentiality	Not Available

8.1. Authentication Security

Authentication Security is only applicable to Iridium Subscriber Units (ISUs) that utilize a SIM card (i.e. the Iridium 9523.) The 9603 and 9602 SBD transceivers do not utilize a SIM card. The Iridium authentication process is adapted without change directly from the GSM specifications. The GSM algorithm A3 is used to encrypt authentication information transmitted over the air interface.

- Authentication encryption - designed to prevent ISU cloning fraud
- GSM encryption algorithm A3 is executed on SIM card to generate Signed Result (SRES) response based on the following inputs
  - Secret key parameter stored in SIM card
  - RAND parameter supplied by network

8.2. Iridium Channel Security

SBD uses the signaling channel and is afforded some security by limited distribution of the air interface and feeder link interface specifications. The Iridium Air Interface Specification is made available only to Iridium Subscriber Unit (ISU) manufacturers. Feeder link interface specifications are not distributed outside of the original manufacturer.

Figure 8-1 identifies the opportunities for surreptitious monitoring of Iridium bearer channels. An eavesdropper could, in principle, monitor L-band uplink and downlink channels, or K-band uplink and downlink feeder link channels.

Table 8-2 Iridium Channel Uplinks & Downlinks

Iridium Channel Uplinks & Downlinks		
Connection	**L-Band Channels**	**K-Band Channels**
Uplink	Uplink, from ISU to Space Vehicle (SV)	Uplink, from gateway to Space Vehicle (SV)
Downlink	Downlink, from SV to ISU	Downlink, from SV to gateway

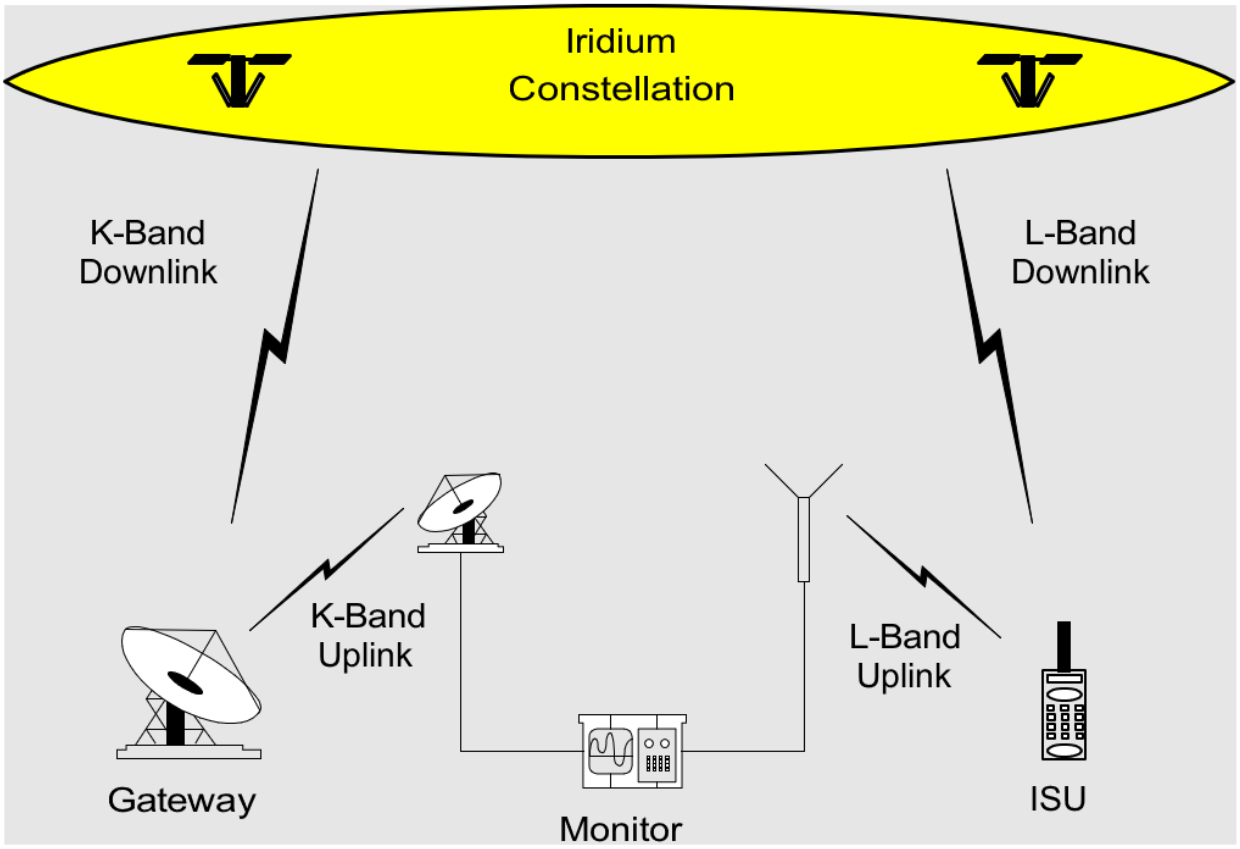


Figure 8-1 Opportunities for Surreptitious Monitoring

8.3. L-Band Channel Security

To successfully monitor an L-band channel, an eavesdropper must be located within the transmit range of the ISU being monitored, approximately 10 to 30 km from the transmitting ISU. ISU downlink L-Band transmissions could be received over a much wider area. A single SV beam covers an area of about 400 km in diameter. If the eavesdropper is within the coverage area of a common beam, downlink L-Band transmissions could be received.

Fortunately, the complexity of the Iridium air interface should make the challenge of developing an Iridium LBand monitoring device very difficult and probably beyond the reach of all but the most determined adversaries. Among the complications are:

- Large, continually changing Doppler shifts
- Frequent inter-beam and inter-SV handoffs
- Time-division multiplexed burst mode channels
- Complicated modulation, interleaving and coding

8.4. K-Band Channel Security

To successfully monitor a K-band feeder link channel, a sophisticated monitoring device must be located in the general proximity of an Iridium gateway. The receiver must have a high-gain antenna capable of tracking SVs as they move from horizon to horizon.

Again, the complexity of the feeder link interface poses a formidable technical challenge for prospective eavesdroppers. The cost of the monitoring device alone would be a strong deterrent. Among the technical complications are

- Large, continually changing Doppler shifts
- High capacity, 3.072 Mbps channels
- High-gain tracking antenna required
- Must reacquire new SV every 10 minutes

8.5. Gateway to Vendor Application

While this document focuses on the Iridium network, security should be looked at from an end-to-end solution perspective. SBD communications to and from the Iridium Gateway can be protected by two additional cost items:

- Virtual Private Network and/or
- Private leased line communication

If using Iridium CloudConnect SBD, Amazon Web Services offers a number of security features and solutions that can be viewed in more detail on the Iridium CloudConnect GitHub page: https://github.com/aws-samples/aws-iot-iridium-satellite.

8.6. Additional Considerations

Depending on the level and sensitivity of the information being communicated the application developer may require additional security. Any additional security measure would require encrypting the information before transmitting to the destination point. This is referred to generically as application level encryption and requires the developer to select and implement an encryption method that provides the required level of security for the application. Any increase in the size of the actual information being sent due to the encryption is not distinguished by the Iridium network from normal user data and the Iridium network will rate the total size of the data message sent.

9. Basic Troubleshooting Steps

The following steps should be taken when experiencing issues with an Iridium SBD transceiver:

- In general, when in early stages of development, Iridium recommends usage of its provided developer kits. Assistance from Iridium support is limited when using third-party hardware.
- Verify that the power requirements specified in the transceiver's developer's guide are met.
- Check that the transceiver has an active and correctly configured serial connection.
- Restart the transceiver.
- Verify that the most recent version of available firmware is installed, if not then update the firmware. Firmware version can be checked with +CGMR.
- Check the transceiver's provisioning. Verify that it has:
  - An active contract
  - SBD Ring Alerts enabled
  - In the case of the 9523, an activated and properly provisioned SIM card.
  - 9602 and 9603 do not require SIM cards
- Check antenna alignment. Best practices for antenna placement include:
  - No more than 3 dB of loss between the antenna and the transceiver
  - The antenna should have a 360 degree view of the sky
  - No obstructions above 8 degrees above the horizon
- Signal strength should be checked before each SBD session using +CSQ.
  - Signal strength should be 2 or higher to ensure the successful completion of an SBD session.
- SBD sessions should not be initiated more than every 60 seconds.

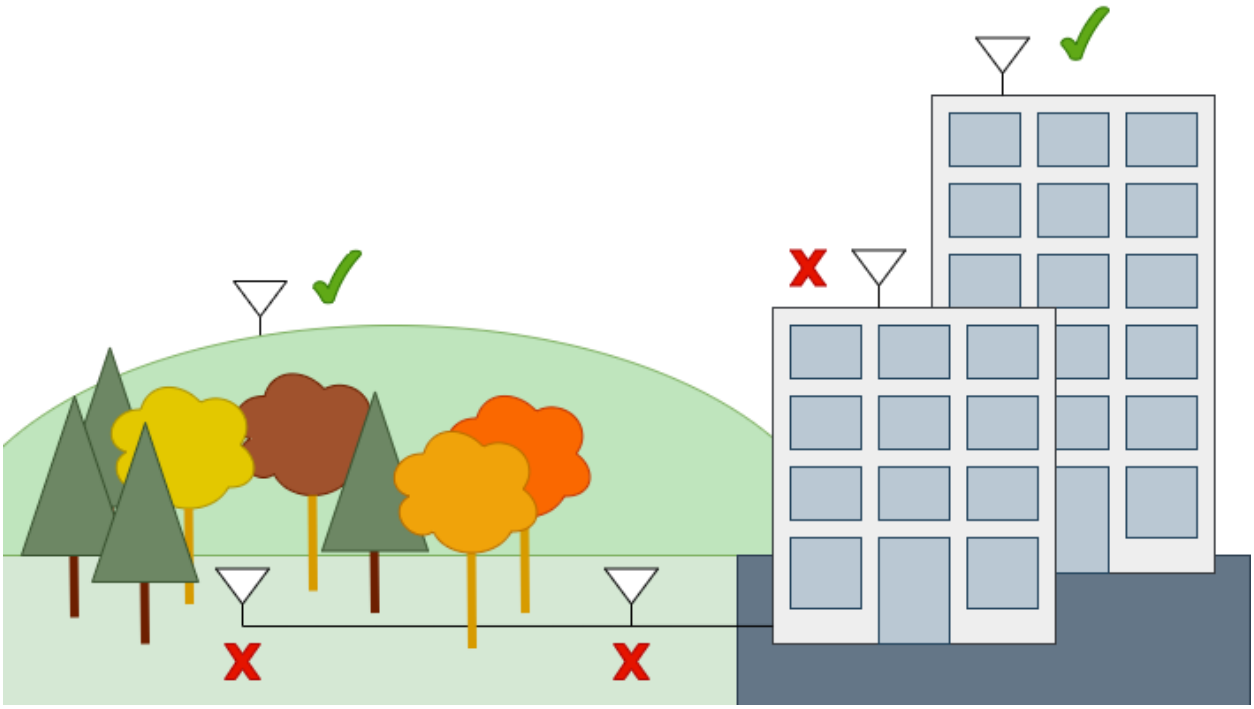


Figure 9-1 Optimal antenna placement

Iridium recommends that development, demonstration and test platforms have high quality installations with optimal line of sight conditions. Having an ideally located antenna removes the possibility that poor signal strength causes application issues and enables more rapid application debugging. In addition, SBD best practices should be observed in all stages of development.

9.1. Transmissions from Deactivated Units

Prior to deactivating a unit on the Iridium network, transmissions and network access requests from SBD devices must be disabled. In some cases, customers might not be able to access devices to disable transmissions from certain inactive SBD devices, particularly for devices located in remote or inaccessible areas. 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. Any Iridium device disabled in this manner can't be reactivated remotely via the Iridium network. Customers will need to have physical access to the device and/or an alternative mechanism such as cellular or Wi-Fi built into their application.

10. Iridium Time Re-Epoch Advisory

As part of standard network operations, the Iridium network periodically resets the L-Band system time through a process called Iridium Time (IRT) Re-Epoching. The IRT is a 32-bit counter (known as L-Band Frame Number (LBFN)), stored as a 32-bit integer, and expressed in 90-millisecond counts from an epoch.

The IRT is critical for synchronizing all Iridium subscriber units/equipment (ISUs/ISE) and transceivers within the Iridium network. Due to the IRT periodic resets, there are risks associated with using LBFN in application code. Iridium highly advises developers not to use LBFN as a gating mechanism nor to calculate datetime. Gating mechanisms refer to control structures or conditions that regulates access to a resource, function, or process, ensuring that execution proceeds only when specific criteria are met. The use of LBFN as a gating mechanism or to calculate datetime may result in unexpected behavior, time synchronization issues, and increased vulnerability of their devices during periodic re-epoch events.

LBFN is exposed with the following AT commands:

AT-MSGEO	Request Geolocation
AT-MSGEOS	Request Geolocation, spherical co-ordinates
AT-MSSTM	Request System Time
AT+CRISX	Ring Indication Status
AT+CCLK	Real-Time Clock (Deprecated)

Developers should investigate if any of these commands are used and determine how LBFN is used in their application code.

10.1. Iridium Half-Time

The IRT is a 32-bit counter. Iridium Half-Time occurs when IRT reaches 2^{31} (half of 2^{32}). A 32-bit integer can be represented in two ways: unsigned and signed.

An unsigned 32-bit integer only stores non-negative values, ranging from 0 to $2^{32}-1$ (0 to 4,294,967,295).

A signed 32-bit integer uses one bit for the sign (positive or negative) and the remaining 31 bits for the value, resulting in a range from -2^{31} to $2^{31}-1$ (-2,147,483,648 to 2,147,483,647).

If LBFN is being used, developers should investigate and ensure that LBFN is stored as an unsigned 32-bit integer (UINT32) in their application code. Applications that store IRT as a signed integer will experience a rollover to a negative time value, leading to disruptions in functionality.

11. Dual Mode Operation:

Software SG25001 or later enables dual mode operation between Burst or SBD. The transceiver operates in the mode selected only. It is important to understand that every time the 9602 or 9603 is turned on or rebooted, the transceiver will be set into SBD mode. A complete description of the command is available in the *Iridium 9602 and 9603 AT Command Reference Guide*.

Appendix A: Definitions, Acronyms, and Abbreviations

Term	Description
API	Application Programming Interface
ATC	AT Command
CDR	Call Detail Record
DB	Data Base
DMO	DirectIP Mobile Originated
DMT	DirectIP Mobile Terminated
DSC	Delivery Short Code
DTE	Data Terminal Equipment
ECS	ETC Communications Subsystem
EMO	Email Mobile Originated
EMT	Email Mobile Terminated
ESS	ETC SBD Subsystem
ETC	Earth Terminal Controller
ETS	ETC Transmission Subsystem
FA	Field Application
GPS	Global Positioning System
IE	Information Element
IEI	Information Element Identifier
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
ISU	Iridium Subscriber Unit
LBT	L-Band Transceiver
Message	The complete data transfer between the Vendor Application and the Iridium Gateway including a head, optional sets of information and the payload to be transmitted over the air.
MIME	Multipurpose Internet Mail Extensions
MO	Mobile Originated

Term	Description
MOMSN	Mobile Originated Message Sequence Number
Mobile Originated Buffer	This is the buffer in the ISU in which an SBD message to be sent from the ISU to the Iridium Gateway will be stored.
MSN	Message Sequence Number
MT	Mobile Terminated
MTMSN	Mobile Terminated Message Sequence Number
Mobile Terminated Buffer	This is the buffer in the ISU in which an SBD message sent from the Iridium Gateway to the ISU will be stored.
Payload	The actual user data to be transmitted over the Iridium network
PIN	Personal Identification Number
SBD	Short Burst Data
SIM	Subscriber Identity Module
SPNet Pro	Iridium's proprietary provisioning tool for contracted business partners
SEP	SBD ETC Processor
SPP	SBD Post Processor
UTC	Coordinated Universal Time
VA	Vendor Application
GSS	Iridium Gateway

Referenced Documents

For the latest Iridium partner documentation, log in to the Iridium for Partners (IFP) website at https://www.iridium.com/login and then go to the Resources section.

No.	Document	Description
1	IRDM-1023-ICD-014 (9602 and 9603) IRDM-1023-ICD-015 (9523)	*Iridium 9602 and 9603 AT Command Reference Guide*
2	IRDM-1023-UDOC-002	*Iridium 9602N Transceiver Developer Guide*
3	IRDM-1023-UDOC-003	*Iridium 9603N Transceiver Developer Guide*
4	IRDM-1023-UDOC-006	*Iridium 9523N Transceiver Developer Guide*
5	https://github.com/aws-samples/aws-iot-iridium-satellite	Iridium CloudConnect GitHub
6	https://www.iridium.com/iridium-sbd-dip-request-form/	DirectIP Whitelisting Form

Email RFC Compliance

The following is a list of the principle relevant RFC's governing the e-mail messages received and sent by the EmailMT process. All e-mail clients connected to EMT are expected to conform to these standards, and EMT conforms to the relevant standards when sending diagnostic e-mails in response to SBD messages.

- 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
- 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
- 2047: Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text
- 2048: Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
- 2049: Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
- 2183: Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field
- 2231: MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations (Obsoletes RFC 2184)
- 2821: Simple Mail Transfer Protocol (Obsoletes RFC 821)
- 2822: Internet Message Format (Obsoletes RFC 822)

EAR Controlled. See legal disclaimer page for use and disclosure statement.

Iridium Proprietary Business Information