

Using TFTs on BGAN

Version 01
12.06.06

www.inmarsat.com/bgan

Whilst the information has been prepared by Inmarsat in good faith, and all reasonable efforts have been made to ensure its accuracy, Inmarsat makes no warranty or representation as to the accuracy, completeness or fitness for purpose or use of the information. Inmarsat shall not be liable for any loss or damage of any kind, including indirect or consequential loss, arising from use of the information and all warranties and conditions, whether express or implied by statute, common law or otherwise, are hereby excluded to the extent permitted by English law. INMARSAT is a trademark of the International Mobile Satellite Organisation, Inmarsat LOGO is a trademark of Inmarsat (IP) Company Limited. Both trademarks are licensed to Inmarsat Global Limited. © Inmarsat Global Limited 2006. All rights reserved.



Contents

1.0.	Introduction	3
1.1.	About this guide	3
1.2.	Other sources of information	3
2.0.	Introduction to TFTs	4
2.1.	What is a TFT?	4
3.0.	The structure of a TFT	5
3.1.	TFT parameters	5
3.2.	Parameter descriptions	5
3.3.	Evaluation precedence index examples	7
3.4.	TFT examples	9
4.0.	TFTs supplied with BGAN LaunchPad	10
4.1.	FTP	10
4.2.	Win Media	10
4.3.	Real Media	11
4.4.	Quick Time Media	11
4.5.	Quick Link	11
4.6.	Streambox	12
5.0.	Writing your own TFTs	13
6.0.	Troubleshooting	14



I.0. Introduction

I.1. About this guide

This document introduces traffic flow templates (TFTs) and explains how they are used on the BGAN network.

It is intended for experienced end-users, Distribution Partners, Service Providers and anyone who wants to use a BGAN terminal to connect to the BGAN network and use network services. A previous knowledge of satellite communications is useful, but not essential.

The sections include:

- Introduction to TFTs – explains how TFTs are used in BGAN LaunchPad and on the BGAN network.
- The structure of a TFT – lists the parameters that make up a TFT, and gives guidance on the information contained in the .xml file that defines the TFT.
- TFTs supplied with BGAN LaunchPad – lists the pre-configured TFTs supplied with BGAN LaunchPad, and provides information on their characteristics.
- Writing your own TFTs – a brief overview of the factors to consider when creating your own TFTs.
- Troubleshooting – a checklist in case you encounter problems.

I.2. Other sources of information

- This is one of a series of PDF documents in the BGAN Solutions Guide. The Solutions Guide is designed to help you make the most of your BGAN terminal. Other documents in the series are available for download from www.inmarsat.com/bgan. Click on **BGAN support**, then click on **How to guides**.

This Web site also gives further information on the BGAN service, including Industry solutions.

- Refer to “BGAN LaunchPad Help” for details on using BGAN LaunchPad.
-



2.0. Introduction to TFTs

A Traffic Flow Template (TFT), also called an Application Template, is a series of filters that ensure that traffic for a particular application does not have to share a connection with any other traffic. In BGAN LaunchPad, a TFT is associated exclusively with a secondary PDP context, that is with a dedicated streaming connection.

2.1. What is a TFT?

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

If you want to define your own TFT for another application, refer to section 3.0 “The structure of a TFT”.

BGAN LaunchPad supports the following pre-configured TFTs, any one of which can be selected when you configure a dedicated streaming connection:

- FTP
- QuickLink
- QuickTime
- Real Media
- Streambox
- WinMedia

Refer to section 4.0 “TFTs supplied with BGAN LaunchPad” for details.



3.0. The structure of a TFT

This section introduces the parameters that must be defined to create a TFT.

3.1. TFT parameters

The BGAN terminal uses +CGTFT commands to create the filters that define the TFT. (Some terminals also use _ITFT commands.) The commands are stored in an .xml file which is divided into two parts – one for the uplink, and one for the downlink. The parameters for the command are as follows:

```
<TFT>
<TFTNAME></TFTNAME>
<up-link>

  <PACKET-FILTER></PACKET-FILTER>
  <EVALUATION-PRECEDENCE-INDEX></EVALUATION-PRECEDENCE-INDEX>
  <DESTINATION-ADDRESS-AND-SUBNET-MASK></DESTINATION-ADDRESS-AND-
SUBNET-MASK>
  <PROTOCOL-NUMBER></PROTOCOL-NUMBER>
  <DESTINATION-PORT-RANGE></DESTINATION-PORT-RANGE>
  <SOURCE-PORT-RANGE></SOURCE-PORT-RANGE>
  <IPSEC-SECURITY-PARAMETER-INDEX></IPSEC-SECURITY-PARAMETER-INDEX>
  <TYPEOFSERVICE-AND-MASK></TYPEOFSERVICE-AND-MASK>
  <FLOW-LEVEL></FLOW-LEVEL>

</up-link>

<down-link>
  <PACKET-FILTER></PACKET-FILTER>
  <EVALUATION-PRECEDENCE-INDEX></EVALUATION-PRECEDENCE-INDEX>
  <SOURCE-ADDRESS-AND-SUBNET-MASK></SOURCE-ADDRESS-AND-SUBNET-MASK>
  <PROTOCOL-NUMBER></PROTOCOL-NUMBER>
  <DESTINATION-PORT-RANGE></DESTINATION-PORT-RANGE>
  <SOURCE-PORT-RANGE></SOURCE-PORT-RANGE>
  <IPSEC-SECURITY-PARAMETER-INDEX></IPSEC-SECURITY-PARAMETER-INDEX>
  <TYPEOFSERVICE-AND-MASK></TYPEOFSERVICE-AND-MASK>
  <FLOW-LEVEL></FLOW-LEVEL>

</down-link>
</TFT>
```

3.2. Parameter descriptions

<TFTNAME>

The TFT Name can be any meaningful name, for example Win Media etc. If you do not specify a value for the TFT Name, BGAN LaunchPad raises an exception.

Mandatory parameters

The following two parameters must be included in a TFT.

<PACKET-FILTER>

The packet filter index uniquely identifies the filter within a single TFT. The index can be in the range 1 to 8. The index number does not indicate that any filter has precedence over any other,

it is simply used for identification purposes. The same packet filter index cannot be used twice in the same TFT, although it can be used in other TFTs.

<EVALUATION-PRECEDENCE-INDEX>

The evaluation precedence index defines the precedence given to a filter when the GGSN (Gateway GPRS Support Node) receives IP traffic from the Internet and routes it to the terminal. The filter with the precedence index of 0 is the first to be applied, the filter with the precedence index of 1 is next and so on. The lowest possible evaluation precedence index is 255.

The evaluation precedence index must be unique across all active TFTs applied to same APN. If same evaluation precedence index is used by two or more active TFTs on the same APN, the first secondary PDP context can connect, but all subsequent secondary PDP contexts with the same evaluation precedence index will fail.

Refer to section 3.3 “Evaluation precedence index examples” for details on how to use the evaluation precedence index.

NOTE: BGAN LaunchPad is supplied with some pre-configured TFTs, each of which uses a range of evaluation precedence indexes. Note that when one of these TFTs is active, you cannot use the associated indexes with any other active TFT on the same APN. Refer to section 4.0 “TFTs supplied with BGAN LaunchPad” for details on the indexes used.

Other parameters

In addition to the Packet Filter and Evaluation Precedence Index, each TFT must contain at least one of the following parameters. Some parameters are mutually exclusive; the table below shows which parameters can be used together.

For example, if you want to define a “Source address and subnet mask”, and an “IPSec SPI”, the only combination that allows the use of these two parameters together is combination 2. Combination 2 also gives you the option to define “Protocol number” and “Type of service”, if required, but no other parameter is available in this combination.

Examples of each of these combination types are given in section 3.4 “Evaluation precedence index examples”.

Parameter	Combination 1	Combination 2	Combination 3
Destination/Source address and subnet mask	✓	✓	✓
Protocol number	✓	✓	
Destination port range	✓		
Source port range	✓		
IPSec SPI		✓	
Type of service	✓	✓	✓
Flow level			✓



Each of these parameters is described below:

<DESTINATION-ADDRESS-AND-SUBNET-MASK>/

<SOURCE-ADDRESS-AND-SUBNET-MASK>

This is an IPv4 IP address and subnet mask.

If set on the **uplink**, only packets that are addressed to the specified **destination** are accepted by the filter.

If set on the **downlink**, only packets received from the specified **source** are accepted by the filter.

<PROTOCOL-NUMBER>

This is uniquely assigned by the IANA for the protocol being used. TCP is set to 6, and UDP is set to 17. The protocol number determines which protocol is used by the TFT.

<DESTINATION-PORT-RANGE>/<SOURCE-PORT-RANGE>

These parameters require knowledge of ports being used by the selected applications.

For example, Internet Explorer uses ports between 1024 to 5000, and connects to Web Server on port 80. Enter these values as shown below:

<DESTINATION-PORT-RANGE>80 . 80</DESTINATION-PORT-RANGE>

<SOURCE-PORT-RANGE>1024 . 5000</SOURCE-PORT-RANGE>

Note that you must enter the ports as a range, even if there is only one figure.

<IPSEC-SECURITY-PARAMETER-INDEX>

The security parameter index (SPI) is an arbitrary value that identifies which security association to use in communications between two entities, for example between one QoS-managed network and another QoS-managed network. When a network sends a packet that requires IPSec protection, it looks up the security association (SA) in its database, and inserts the SPI into the IPSec header. The receiving device looks up the SA in its database by destination address and SPI, and processes the packet. The SPI can be any value between 256 and 16639.

<TYPEOFSERVICE-AND-MASK>

Type of Service (TOS) is an 8-bit field in a packet header, with associated mask, that is used to define Quality of Service (QoS). If you do not want to use this parameter, set it to 0 . 0.

<FLOW-LEVEL>

This is an IPv6 flow label, and therefore not used in BGAN. Leave this parameter blank.

Refer to section 3.4 “TFT examples” for examples on how and when to use each of these parameters.

3.3. Evaluation precedence index examples

The evaluation precedence index defines the order in which the filters defined in the TFT are applied to packets.

In this example, Context ID (CID) 1 is the primary PDP context, over a standard IP connection. You have defined two TFTs over secondary PDP contexts, as follows:

- CID 2 is for RTSP traffic routed via a 64kbps streaming connection.
- CID 3 is for UDP traffic routed via a 32kbps streaming connection.



You define the evaluation precedence indexes as shown in the following table:

CID	2	2	3
Packet Filter ID	1	2	1
Evaluation precedence index	0	1	2
Protocol	17	6	17
Port	1024-5000	554	

In this example, packets are filtered as follows:

- First, the packets are tested by evaluation precedence index 0, which checks for UDP packets (protocol number 17), in the port range 1024–5000, and routes those that pass the filter.
- Second, remaining packets are tested against evaluation precedence index 1, which checks for TCP packets (protocol number 6), on port 554, and routes those that pass the filter.
- Third, remaining packets are tested against evaluation precedence index 2, which checks for remaining UDP packets (protocol number 17), and routes those that pass the filter.

Any packets which do not match any of the above filters are routed to the standard IP connection.

This is an example of how evaluation precedence indexes can be assigned to filter packets in a logical sequence. Note that the CID identifier and the packet filter ID do not affect the order in which filters are applied. The evaluation precedence index always has priority. For this reason, the application of evaluation precedence index requires careful consideration.

One example of how the same filters could be applied in an illogical sequence is shown in the following table:

CID	2	2	3
Packet Filter ID	1	2	1
Evaluation precedence index	2	1	0
Protocol	17	6	17
Port	1024-5000	554	

In this example, the packets would be filtered as follows:

- First, the packets are tested by evaluation precedence index 0, which checks for UDP packets (protocol number 17), and routes those that pass the filter.
- Second, remaining packets are tested against evaluation precedence index 1, which checks for TCP packets (protocol number 6), on port 554, and routes those that pass the filter.
- Third, remaining packets are tested against evaluation precedence index 2, which checks for remaining UDP packets in the port range 1024–5000, and routes those that pass the filter.

Note that in this scenario, evaluation precedence index 2 would never be applied, as all UDP packets have already passed the filter defined in evaluation precedence index 0.



It is important, therefore, that an evaluation precedence index with a high priority applies more rigorous filtering on packets than an evaluation precedence index with a lower priority.

3.4. TFT examples

The following are examples of different types of TFT packet filter.

Multi-field classification

In a multi-field classification, the packet filter consists of a number of packet header fields. For example, to define a packet filter on the downlink where:

- The packet filter index is 1.
- The evaluation precedence index is 0.
- The packet source is 172.168.8.0 (subnet mask 255.255.255.0).
- The protocol type is TCP (6).
- The destination port is 5003.

enter the following (the parameters after destination port are not defined in the following example):

```
+CGTFT=1,1,0,172.168.8.0.255.255.255.0,6,5003.5003,,,,,
```

TOS-based classification

In a TOS-based classification, the packet filter consists of only the TOS octet coding. For example, to define a packet filter where:

- The packet filter index is 3.
- The evaluation precedence index is 0.
- The type of service is 00101000 (binary), entered as 40 (decimal).
- The type of service mask is 11111100 (binary), entered as 252 (decimal).

enter the following (the parameters other than those listed above are not defined in the following example):

```
+CGTFT=1,3,0,,,,,040.252,,
```

Multi-field classification for IPSec traffic

In a multi-field classification of IPSec traffic, the packet filter contains the Security Parameter Index (SPI) instead of port numbers that are not available due to encryption. For example, to define a packet filter where:

- The packet filter index is 4.
- The evaluation precedence index is 0.
- The protocol number is 50. (This is protocol number for ESP, the IPSec protocol).
- The SPI is 0x0F80F000.

enter the following (the parameters other than those listed above are not defined in the following example):

```
+CGTFT=1,4,0,,50,,,0F080F000,,,
```



4.0. TFTs supplied with BGAN LaunchPad

There are a number of TFTs supplied with BGAN LaunchPad. When you configure a dedicated streaming connection, you can choose one of these TFTs, along with other connection and routing options. When you then open the dedicated streaming connection, all traffic for that application is transferred over a secondary PDP context.

The following TFTs are supplied with BGAN LaunchPad:

- FTP
- QuickLink
- QuickTime
- Real Media
- Streambox
- WinMedia

The characteristics of each are described in the following sections. Note that a TFT defines the QoS for the application, and defines the filters that will be used over secondary PDP contexts.

4.1. FTP

Purpose	This TFT is used with an FTP application.
Evaluation Precedence Index	1 (Index 1 must not be used with any other active TFT on the same APN)
Protocols	TCP
Ports	TCP (20.21) Range

4.2. Win Media

Purpose	Win Media TFT is used with the Windows Media Player application.
Evaluation Precedence Index	2.3.4.5.6 (This range must not be used with any other active TFT on the same APN)
Protocols	RTSP over TCP RTSP over UDP MMS over TCP MMS over UDP HTTP (currently disabled. If required, can be enabled)
Ports	RTSP over TCP (554) RTSP over UDP (5004.5005) Range MMS over TCP (1755) MMS over UDP (1024.5000) Range HTTP (80)



4.3. Real Media

Purpose	Real Media TFT is used with the Real Media Player application.
Evaluation Precedence Index	7.8.9 (This range must not be used with any other active TFT on the same APN)
Protocols	RTSP over TCP RTSP over UDP
Ports	RTSP over TCP (554) RTSP over TCP (7070.7071) Range RTSP over UDP (6770.7070) Range

4.4. Quick Time Media

Purpose	Quick Time Media TFT is used with the Quick Time application.
Evaluation Precedence Index	10.11.12 (This range must not be used with any other active TFT on the same APN)
Protocols	RTSP over TCP RTSP over UDP HTTP (currently disabled. If required, can be enabled)
Ports	RTSP over TCP (554) RTSP over UDP (7070) HTTP (80)

4.5. Quick Link

Purpose	Quick Link TFT is used with the Quick Link application.
Evaluation Precedence Index	13.14.15.16.17.18 (This range must not be used with any other active TFT on the same APN). 19.20.21.22 (extra range for further requirements. This range must not be used with any other active TFT on the same APN).
Protocols	RTSP over TCP RTSP over UDP TCP HTTP (currently disabled. If required, can be enabled)
Ports	TCP (21.22) Range RTSP over TCP (7070.7071) Range RTSP over TCP (8000.8050) Range RTSP over UDP (7070.7071) Range HTTP (80)



4.6. Streambox

Purpose	Streambox TFT is used with the Streambox application.
Evaluation Precedence Index	22.23 (This range must not be used with any other active TFT on the same APN) 24.25.26.27 (extra range for further requirements. This range must not be used with any other active TFT on the same APN).
Protocols	UDP
Ports	UDP (1700.4199) Range



5.0. Writing your own TFTs

If required you can write your own TFTs, using the structure and parameters defined in section 3.0 “The structure of a TFT”. Note the following:

- The Evaluation Precedence Index must be unique for an active TFT on the APN. If you duplicate an existing Evaluation Precedence Index, only the first secondary PDP context to use this Index can open. All other secondary PDP contexts with this Index will fail. Refer to section 4.0 “TFTs supplied with BGAN LaunchPad” for details on the ranges already assigned.
- The TFT defines the filters that allow traffic that matches the filters to be routed on a particular PDP context, and given a different QoS to traffic on other PDP contexts. To maximize the efficiency of your TFTs, make sure that you give filters a priority that ensures that packets are routed effectively.
- If you have defined a Protocol Number, it must be set to the protocol that you are using – either 6 for TCP, or 17 for UDP.

For further information on defining TFTs, refer to the 3rd Generation Partnership Project (3GPP) web site at www.3gpp.org.



6.0. Troubleshooting

If problems occur when you try to use a TFT, refer to the following check list.

1. Check the `<EVALUATION-PRECEDENCE-INDEX>` and ensure that it is unique to the TFT, if other TFTs are active on this APN.
2. Check the `<PACKET-FILTER>` and ensure that it is not duplicated in the same TFT. (Note that another TFT can have same Packet Filter ID.)
3. Check that the `<DESTINATION-PORT-RANGE>` or `<SOURCE-PORT-RANGE>` is set as a range in the format `<start> . <end>`. If the port is a single number, enter it twice in this format, eg `80 . 80`.
4. Check that all tags in the .xml file are in upper case letters.
5. Check the application that is using the TFT is properly configured. For example, TFTs are configured to use specific ports, and the application may work with different port.
6. Check that data is being transferred over the secondary PDP context, by using BGAN LaunchPad to ensure that the appropriate Dedicated Streaming IP connection is open. The TFT may appear to be operating if data is being transferred, but it may be using the Standard IP connection.
7. Check which ports are being used by an application using a network monitoring tool, such as TCPview.

If the problem persists, the TFT may not be the cause. You may, for example, want to check the application using the TFT to ensure it is configured correctly.
