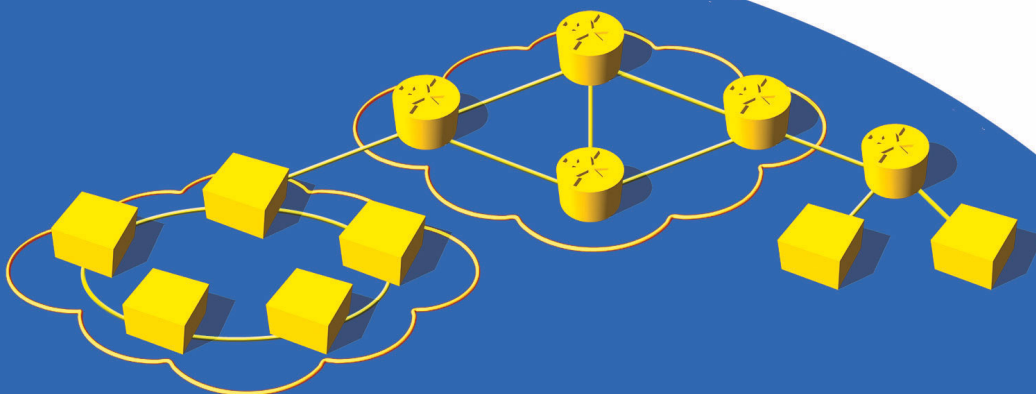


## Technical Note #18

# Data Integrity on TeraMetrics for Version 4.50 or Later Firmware

April 2004



## **Spirent Communications, Inc.**

26750 Agoura Road  
Calabasas, CA  
91302 USA

### **Support Contacts**

#### **U.S.**

E-mail: [support@spirentcom.com](mailto:support@spirentcom.com)

Web: <http://support.spirentcom.com>

Toll Free: 1-800-SPIRENT (1-800-774-7368)

Phone: + 1 818-676-2616

Fax: +1 818-880-9154

#### **Europe**

E-mail: [support.europe@spirentcom.com](mailto:support.europe@spirentcom.com)

Web: <http://support.spirentcom.com>

Phone: +33 (0) 1 61 37 22 70

Fax: +33 (0) 1 61 37 22 51

### **Copyright**

© 2004 Spirent Communications, Inc. All Rights Reserved.

All of the company names and/or brand names and/or product names referred to in this document, in particular, the name "Spirent" and its logo device, are either registered trademarks or trademarks of Spirent plc and its subsidiaries, pending registration in accordance with relevant national laws. All other registered trademarks or trademarks are the property of their respective owners. The information contained in this document is subject to change without notice and does not represent a commitment on the part of Spirent Communications. The information in this document is believed to be accurate and reliable, however, Spirent Communications assumes no responsibility or liability for any errors or inaccuracies that may appear in the document.

### **Limited Warranty**

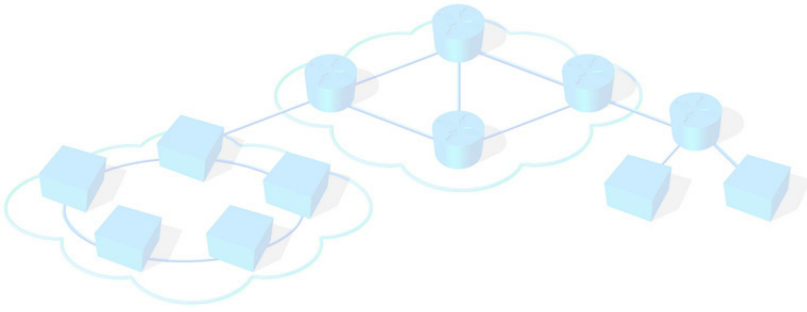
Spirent Communications, Inc. ("Spirent") warrants that its Products will conform to the description on the face of order, that it will convey good title thereto, and that the Product will be delivered free from any lawful security interest or other lien or encumbrance.

Spirent further warrants to Customer that hardware which it supplies and the tangible media on which it supplies software will be free from significant defects in materials and workmanship for a period of twelve (12) months, except as otherwise noted, from the date of delivery (the "Warranty Period"), under normal use and conditions.

To the extent the Product is or contains software ("Software"), Spirent also warrants that the Software, if properly used by Licensee in accordance with the Software License Agreement, shall operate in material conformity with the specification for such Software for a period of ninety (90) days from the date of delivery (the "Warranty Period"). Spirent does not warrant that the functions contained in the Software will meet a specific requirement or that the operation will be uninterrupted or error free. Spirent shall have no warranty obligations whatsoever with respect to any Software which has been modified in any manner by Customer or any third party.

Defective Products and Software under warranty shall be, at Spirent's discretion, repaired or replaced or a credit issued to Customer's account for an amount equal to the price paid for such Product provided that: (a) such Product is returned to Spirent after first obtaining a return authorization number and shipping instructions, freight prepaid, to Spirent's location in the United States; (b) Customer provides a written explanation of the defect or Software failure claimed by Customer; and (c) the claimed defect actually exists and was not caused by neglect, accident, misuse, improper installation, improper repair, fire, flood, lightning, power surges, earthquake, or alteration. Spirent will ship repaired Products to Customer, freight prepaid. Except as otherwise stated, any claim on account of defective materials or for any other cause whatsoever will conclusively be deemed waived by Customer unless written notice thereof is given to Spirent within the Warranty Period. Spirent reserves the right to change the warranty and service policy set forth above at any time, after reasonable notice and without liability to Customer.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY EXCLUDED, AND THE LIABILITY OF SPIRENT, IF ANY, FOR DAMAGE RELATING TO ANY ALLEGEDLY DEFECTIVE PRODUCT SHALL BE LIMITED TO THE ACTUAL PRICE PAID BY THE CUSTOMER FOR SUCH PRODUCT. THE PROVISIONS SET FORTH ABOVE STATE SPIRENT'S ENTIRE RESPONSIBILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY BREACH OF ANY WARRANTY.



# Data Integrity on TeraMetrics

---

This Technical Note provides an introduction to the Data Integrity function when using TeraMetrics version 4.50 or later firmware.

## In this document...

- [Introduction . . . . 2](#)
- [Module Information . . . . 2](#)
- [Design Principles . . . . 3](#)
- [Transmit Configuration . . . . 4](#)
- [Receive Configuration . . . . 4](#)
- [Counter Interpretation and Results . . . . 5](#)
- [Capture Information . . . . 5](#)
- [More Details on Rx Functionality . . . . 5](#)
- [Important Information . . . . 6](#)

## Introduction



**Important:** This Technical Note applies to TeraMetrics version 4.50 or later firmware. For information regarding version 4.30 or earlier firmware, refer to *Technical Note #16, Data Integrity on TeraMetrics*.

The Data Integrity function allows the SmartBits modules to send and receive a frame with a marker, called the Data Integrity marker, as an additional means of verification that the user payload was received correctly. This feature is used to determine if packet corruption occurred internal to a router where the packet is not protected with a Layer 2 CRC.

The Data Integrity function requires that the configuration be set up in a specific manner to operate properly. This Technical Note provides this configuration information for the SmartBits modules and provides answers to frequently asked questions regarding the Data Integrity function.

## Module Information



**Note:** The FBC-3601A and FBC-3602A modules are supported only in SmartLibrary.

The Data Integrity function applies only to the following SmartMetrics and TeraMetrics modules:

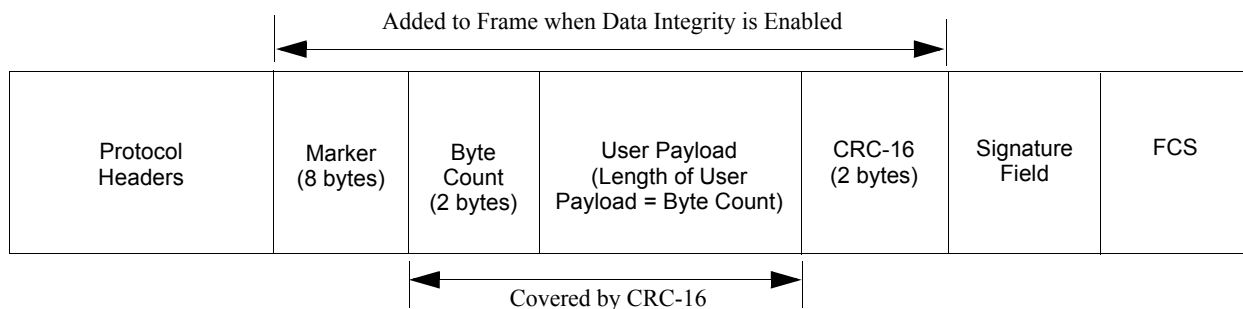
- FBC-3601A Fibre Channel 1G, 2-port, SmartMetrics
- FBC-3602A Fibre Channel 1G and 2G, 2-port, SmartMetrics
- LAN-3300A 10/100/1000Base-T Ethernet, Copper, 2-port, SmartMetrics
- LAN-3301A 10/100/1000Base-T Ethernet, Copper, 2-port, TeraMetrics
- LAN-3302A 10/100Base-T Ethernet, Copper, 2-port, TeraMetrics
- LAN-3306A 10/100Base-TX Ethernet, Copper, 4-port, TeraMetrics XD
- LAN-3310A 1000Base-X Ethernet, GBIC, 2-port, SmartMetrics
- LAN-3311A 1000Base-X Ethernet, GBIC, 2-port, TeraMetrics
- LAN-3320A 10/100/1000 Mbps and Gigabit Ethernet Fiber, 2-port, SmartMetrics XD
- LAN-3321A 10/100/1000 Mbps and Gigabit Ethernet Fiber, 2-port, TeraMetrics XD
- LAN-3324A 10/100/1000 Mbps and Gigabit Ethernet Fiber, 4-port, SmartMetrics XD
- LAN-3325A 10/100/1000 Mbps and Gigabit Ethernet Fiber, 4-port, TeraMetrics XD
- LAN-3327A 10/100/1000 Mbps and Gigabit Ethernet Fiber, 1-port, TeraMetrics XD
- POS-3504As POS OC-48c, 1-port, single mode, 1310nm, SmartMetrics
- POS-3504Ar POS OC-48c, 1-port, single mode, 1550nm, SmartMetrics

- POS-3505As POS OC-48c, 1-port, single mode, 1310nm, TeraMetrics
- POS-3505AR POS OC-48c, 1-port, single mode, 1550nm, TeraMetrics
- POS-3510A POS OC-3c/OC-12c, 2-port, multi-mode, 1300nm, SmartMetrics
- POS-3510As POS OC-3c/OC-12c, 2-port, single mode, 1310nm, SmartMetrics
- POS-3511A POS OC-3c/OC-12c, 2-port, multi-mode, 1300nm, TeraMetrics
- POS-3511As POS OC-3c/OC-12c, 2-port, single mode, 1310nm, TeraMetrics
- POS-3518As POS OC-192c, 1-port, 2-slot, single mode, 1310nm, SmartMetrics
- POS-3518AR POS OC-192c, 1-port, 2-slot, single mode, 1550nm, SmartMetrics
- POS-3519As POS OC-192c, 1-port, 2-slot, single mode, 1310nm, TeraMetrics
- POS-3519AR POS OC-192c, 1-port, 2-slot, single mode, 1550nm, TeraMetrics
- XLW-3720A 10Gbps Ethernet, Optical, XENPAK, 1-port, 2-slot SmartMetrics
- XLW-3721A 10Gbps Ethernet, Optical, XENPAK, 1-port, 2-slot TeraMetrics

## Design Principles

The SmartBits modules listed above use the Trigger logic on the receive side to recognize the `_NETCOM_` pattern in the frame and start Data Integrity calculations. These SmartBits modules do not “scan” packet contents for the Data Integrity marker. Instead, the pattern matching logic in the Rx Trigger circuit examines a specified byte offset in the frame to determine if a marker is present or not.

A Data Integrity frame has a marker that displays as `_NETCOM_` in ASCII immediately following the last protocol header. In hexadecimal, the marker is `5f 4e 45 54 43 4f 4d 5f`. Immediately after the marker, there is a 2-byte Byte Count field, the User Payload, and the CRC-16, followed by the Signature Field and the FCS for the frame. The format shown below is the definition of Data Integrity within a SmartMetrics or TeraMetrics frame.



## Transmit Configuration

To transmit Data Integrity frames for a stream on a TeraMetrics module, select **Enable Data Integrity** in either SmartWindow or SmartLibrary.



### Important:

- When you configure streams in SmartWindow 8.00, the streams are set to transmit the Data Integrity marker by default.
- Data Integrity can be *Enabled* or *Disabled* in the Streams Configuration window or you can select a stream, choose **edit**, and check the **Data Integrity** box.
- Only frames that contain the Signature Field can have Data Integrity enabled. This means that Data Integrity works only when the module is in SmartMetrics mode and the Signature Field is enabled.
- The modules statically calculate TCP checksums during stream configuration, prior to real time generation of packets. Data Integrity calculations are performed in real time. Therefore, the Data Integrity feature cannot be used with the TCP protocol. Data Integrity does work with IP and UDP protocol.



**Note:** TeraMetrics modules do not support error injection in this feature. However, it is possible to send errored Data Integrity frames using the custom protocol by imitating a faulty Data Integrity frame.

When Data Integrity is enabled, it modifies the following in the modules:

- Places the start of the Data Integrity immediately after the protocol headers. This start position can vary, depending on the specifics of the protocol stack in the packet.
- Includes the marker, length, and CRC-16 fields.

## Receive Configuration

To count or measure Data Integrity frames on a TeraMetrics module, you must first set a receive trigger on the Data Integrity marker.

To set a receive trigger on the Data Integrity marker using SmartWindow or SmartLibrary, set trigger 1 to match the last six bytes of the 8-byte Data Integrity marker. The byte offset for the trigger must be set to point to the **E** in `_NETCOM_` and the trigger value should be set to `ETCOM_` (hexadecimal 45 54 43 4f 4d 5f).

For example, when receiving in an Ethernet frame with an IP header only, the offset should be set to byte 36, corresponding to the E (ASCII 45).



### Important:

- There are two receive triggers: Rx Trigger 1 and Rx Trigger 2.
- Receive Trigger 1 must be correctly configured to recognize the Data Integrity marker.

- When Receive Trigger 1 is used for Data Integrity marker detection, the other trigger must not interfere. In SmartWindow's Receive Trigger Setup, select **Only trigger 1, ignore trigger 2**.
- A Receive Trigger offset is a static value. It can only point to a fixed number of bytes beyond the beginning of a packet. This is a *per port* parameter. The byte offset of the receive trigger must be based on the received frame type, not the transmitted frame type.

## Counter Interpretation and Results

When the transmit and receive settings are set according to this document, the Data Integrity counter will show Data Integrity errors detected on the receive port. Frames with Data Integrity errors will be counted in the frame receive statistics, both counters and histograms.

## Capture Information

In SmartWindow, select **Capture**, and set *Capture Events* to either **All Frames** or **Data Integrity Errors**. In both capture events, the capture status will display **D** for those frames with Data Integrity errors.

## More Details on Rx Functionality

The trigger/match logic is implemented as described above. However, it conveys only MATCH or NO\_MATCH information. If there is a MATCH, it provides a byte pointer where the match occurred to the Receive Engine.

The Receive Engine performs the following actions for Data Integrity:

- If MATCH = TRUE, then the LENGTH field is used to re-calculate the CRC-16 and is compared to the CRC-16 in the packet.
- If it is a signature frame and the CRC-16 is errored, then the Data Integrity ERROR counter is incremented.
- If it is not a signature frame, then Data Integrity errors are ignored.



**Note:** Data Integrity Check will be enabled in SmartWindow on trigger setup, only when user selects **Only trigger 1, ignore trigger 2**, with a trigger range of **6**, and a trigger pattern of **ETCOM\_** (hexadecimal 45 54 43 4f 4d 5f). Otherwise, no Data Integrity Check will be performed on frames even if other criteria matches.

## Important Information

The following information is important for the operation of Data Integrity:

- There is no *always on* detection of the Data Integrity marker; the Rx trigger must be configured to see the marker.
- Rx Trigger resource is consumed when running Data Integrity tests.
- Since the Alternate Key Feature also consumes the Rx trigger resource, Data Integrity Check will be disabled when the Alternate Key Feature is enabled, regardless of trigger setup.