

GigaSMART Operation Reference Guide

GigaSMART

Product Version: 6.14

Document Version: 1.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.14	1.0	02/25/2026	The original release of this document with 6.14.00 GA.

Contents

GigaSMART Operation Reference Guide	1
Change Notes	3
Contents	4
GigaSMART-Operations-Reference-Guide	7
Work with GigaSMART Operations	7
GigaSMART Licensing	9
Access GigaSMART from GigaVUE-FM	9
Quick Glance- How to Configure a GigaSMART Application	10
Create GigaSMART Operations – A Summary	12
Groups of GigaSMART Engine Ports	13
Reload GigaSMART engine ports in a group	15
How to Use GigaSMART Operations – Example	16

Engine Watchdog Timer in GigaSMART	18
Tunnel Health Checks	19
Configure Hashing	21
GigaSMART Rules and Tips	21
Virtual Ports	23
Virtual Port Rules	23
Create Virtual Port	23
Multiple Virtual Ports for First Level Map	26
Multiple Virtual Port Rules	29
Multiple Virtual Port with Other GigaSMART Applications	30
Virtual Port Statistics	33
Differences in GigaSMART Nomenclature Between the CLI and GigaVUE-FM	34
GigaSMART Operations in Clusters	34
How to Combine GigaSMART Operations	36
How to Read GigaSMART Operations Table	37
Work with GigaSMART Operation Combinations in GigaVUE-FM	38
Supported GigaSMART Operations	39
Supported GigaSMART Operations on GigaVUE HC Series	39
Order of GigaSMART Operations	42
View GigaSMART Statistics	43
Definitions of GigaSMART Statistics	44
NetFlow Monitor Statistics Definitions	44
NetFlow Exporter Statistics Definitions	45
IP Interfaces Statistics Definitions	46
TLS/SSL Application Statistics Definitions	47
ASF Statistics Definitions	48
GigaSMART Group Statistics Definitions	49
GigaSMART Group Flow Ops Report Statistics Definitions	51
Flow Ops Report Statistics Definitions for FlowVUE	51
Flow Ops Report Statistics Definitions for GTP	51
Flow Ops Report Statistics Definitions for GTP Overlap	55
Flow Ops Report Definitions for SIP/RTP Correlation	56
Flow Ops Report Statistics for Passive TLS/SSL Decryption	58

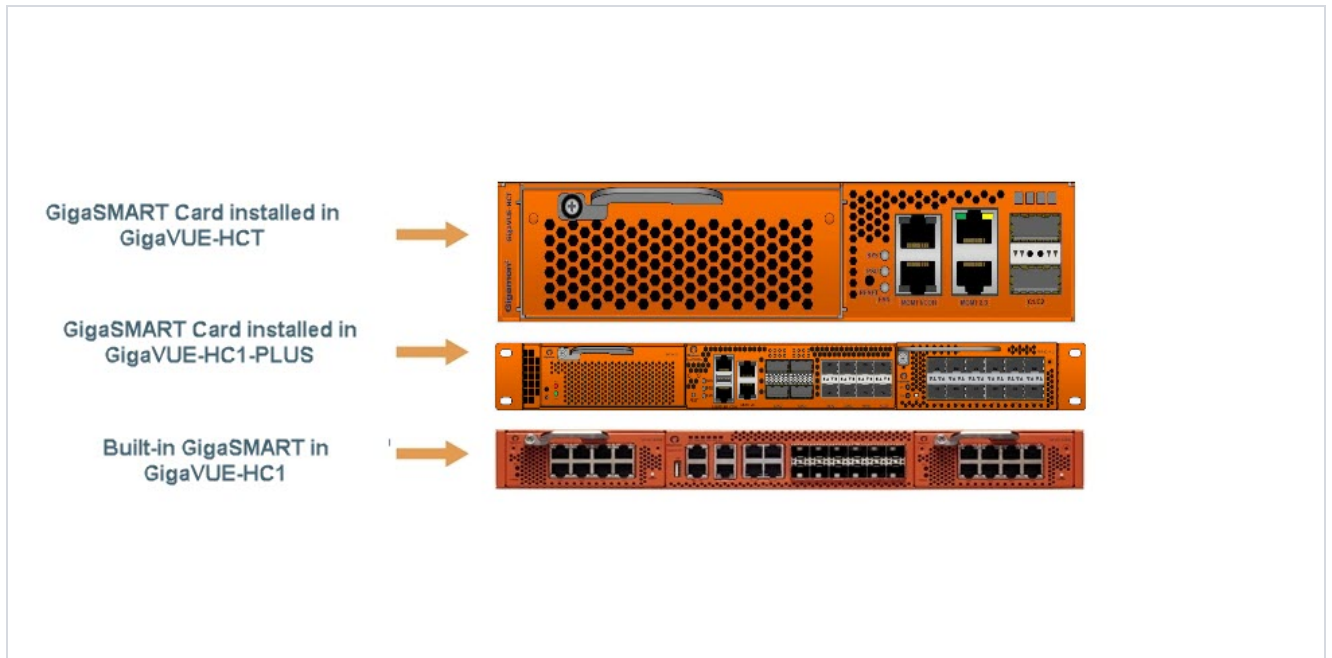
GigaSMART Operations Statistics Definitions	59
Passive TLS/SSL Decryption Statistics Definitions	60
Inline TLS/SSL Decryption Statistics Definitions	61
De-duplication Statistics Definitions	61
ERSPAN Statistics Definitions	62
Tunnel Decapsulation Statistics Definitions	63
Tunnel Encapsulation Statistics Definitions	64
APF Statistics Definitions	67
ASF Statistics Definitions	67
Masking Statistics Definitions	67
Slicing Statistics Definitions	68
Header Stripping Statistics Definitions	68
Generic Header Stripping Statistics Definitions	69
Trailer Statistics Definitions	69
FlowVUE Statistics Definitions	70
NetFlow Statistics Definitions	70
Display GigaSMART Application Resource Usage	71
Overview of GigaSMART Application Resources	72
Resources for Buffer ASF	73
Reload GigaSMART Line Card or Module	73
GigaSMART CPU Utilization Statistics	74
Display GigaSMART CPU Utilization	74
Configure Threshold	75
Configure Threshold Crossing Notification	75
How to Use GigaSMART Trailers	76
Required License: Base	76
Source ID Field	76
Remove GigaSMART Trailers	78
Multiple GigaSMART Trailers and Cascade Connections	80
Interpret GigaSMART Trailer	81
GigaSMART Trailer Reference	81
GigaSMART Trailer Format	81
GigaSMART Trailer Format	81
GigaSMART Trailer TLVs	82
Format of the GIGAMON_SRCID TLV	83

GigaSMART Logs	90
Create GS Log file	90
Delete Log File	91
Additional Sources of Information	92
Documentation	92
How to Download Software and Release Notes from My Gigamon	95
Documentation Feedback	95
Contact Technical Support	96
Contact Sales	97
Premium Support	97
The VÜE Community	97
Glossary	98

GigaSMART-Operations-Reference-Guide

Work with GigaSMART Operations

This chapter describes how to use GigaSMART operations – advanced processing features available for use on GigaVUE-HC1 nodes, GigaVUE-HC1-Plus nodes with GigaSMART modules, and GigaVUE-HCT nodes with SMT-HC1-S module.



Use the **GigaSMART Operations** page to create GigaSMART® operations. The **GigaSMART Operations** page has a name and the details of supported combination of the available GigaSMART applications that you have licensed. Refer to the following sections for details:

- [How to Combine GigaSMART Operations](#) for details on supported combinations of GigaSMART operations.
- [Order of GigaSMART Operations](#) for information on the order in which GigaSMART components are applied in a single operation.
- [Supported GigaSMART Operations](#) for information on supported GigaSMART operations on physical and virtual nodes.
- [Access GigaSMART from GigaVUE-FM](#) for an overview of how to access GigaSMART from GigaVUE-FM.
- [Create GigaSMART Operations – A Summary](#) for an overview of how to create GigaSMART groups and GigaSMART operations from GigaVUE-FM.
- [Engine Watchdog Timer in GigaSMART](#) for configuring Engine Watchdog Timer in GigaSMART.
- [GigaSMART Rules and Tips](#) for rules and notes when using GigaSMART operations.
- [Virtual Ports](#) for overview about Virtual Ports
- [GigaSMART Operations in Clusters](#) for an overview about GigaSMART operations in clusters.
- GigaSMART Operations for comprehensive HowTo's on using all GigaSMART operations.
- [View GigaSMART Statistics](#) for overview about GigaSMART statistics.

The following table details the GigaSMART operation by the type of solution provided:

Application Intelligence	These GigaSMART operations provide network and application visibility to increase the efficiency of security and analytic tools: • Application Intelligence • Application Session Filtering
Subscriber Intelligence	These GigaSMART operations provide network and subscriber visibility to increase the efficiency of network monitoring, security, and customer experience tools: • GTP Correlation • SIP/RTP Correlation • FlowVUE
GigaSMART TLS/SSL Decryption for Inline and Out-of-Band Tools	GigaSMART TLS/SSL Decryption for Inline and Out-of-Band Tools provide network visibility to increase the efficiency of network performance tools.
Traffic Intelligence	These GigaSMART operations provide network visibility to increase the efficiency of network performance tools: • Adaptive Packet Filtering • Advanced Load Balancing • De-duplication • Flow Masking • Header Stripping • Masking • NetFlow Generation • Slicing • SSL/TLS Decryption • PCAPng Application • Tunneling

GigaSMART Licensing

Refer to the GigaVUE Licensing Guide for details.

NOTE: Contact your Gigamon Sales Representative to learn more about the available floating license options for your fabric configuration.

Access GigaSMART from GigaVUE-FM

You can access GigaSMART operations from within GigaVUE-FM, by accessing a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. **GigaSMART** appears in the navigation pane of the device view on supported devices.

To access GigaSMART from the GigaVUE-FM interface:

1. Select **Physical** from the top navigation menu.
2. Select **Physical Nodes** from the side panel. This displays the list of Devices/Cluster Nodes managed by this instance of GigaVUE-FM.
3. Click the Cluster ID of any node to open the node. Once you are in the node, this part of the interface should behave just like HVUE for devices that support GigaSMART. Refer to [About GigaSMART Applications](#).
4. Click **GigaSMART** from the side navigation pane.

Refer to:

- [About GigaSMART Applications](#) for devices that support GigaSMART.
- [Create GigaSMART Operations – A Summary](#) to get started with GigaSMART.
- [GigaSMART Operations](#) to learn how to use GigaSMART operations.

Quick Glance- How to Configure a GigaSMART Application

This section provides you a quick glance on document sections that can get you started on configuring the GigaSMART Applications.

GigaSMART Application	Refer to
Application Intelligence	
Application Intelligence	Create an Application Intelligence Session in Physical Environment
Application Filtering Intelligence	Create Application Filtering Intelligence for Physical Environment
Application Metadata Intelligence	Create Application Metadata Intelligence for Physical Environment
Application Session Filtering	Define ASF Session
Subscriber Intelligence	
GTP Correlation	• GTP Correlation Configuration Examples • GigaSMART GTP Whitelisting and GTP Flow Sampling Examples • Display Flow Ops Reports • GTP Engine Grouping Configuration Examples • GTP Stateful Session Recovery
SIP/RTP Correlation	• Configure SIP/RTP Correlation Engine
FlowVUE	• Configure FlowVUE ◦ FlowVUE Configuration Examples

GigaSMART Application	Refer to
5G CUPS	• 5G Load Balancing • Configure CPN-UPN Communication Solution using Ansible • About Flow Sampling Rules and Maps • Monitoring CUPS Solution (Monitoring of Subscriber Intelligence Solutions)
GigaSMART TLS/SSL Decryption for Inline and Out-of-Band Tools	• Gigamon Inline Solutions
GigaSMART TLS/SSL Decryption for Out-of-Band Tools	• GigaSMART Passive TLS/SSL Decryption
Traffic Intelligence	
GigaSMART Adaptive Packet Filtering (APF)	• Implement APF Through the UI ◦ Adaptive Packet Filtering Examples
Advanced Load Balancing	• Stateful Load Balancing • Stateless Load Balancing • Enhanced Load Balancing
De-duplication	• De-duplication Configuration Steps ◦ Configure GigaSMART Parameters for Packet De-duplication ◦ Example – GigaSMART De-duplication
Flow Masking	• GigaSMART Encapsulated Traffic Performance Enhancement
Header Stripping	• GigaSMART Header Stripping • Generic Header Stripping
Masking	• GigaSMART Masking
NetFlow Generation	• Configure Netflow Generation
Slicing	• Create Advanced Flow Slicing Profile • GigaSMART Packet Slicing
Tunneling	• Custom Tunnel Decapsulation Configuration Example • ERSPAN Tunnel Header Removal ◦ ERSPAN Type III Tunnel Header Removal • GigaSMART IP Encapsulation/Decapsulation (GigaSMART Tunnel) • Configure L2GRE Tunnel Encapsulation and Decapsulation • GigaSMART VXLAN Tunnel Encapsulation • GigaSMART VXLAN Tunnel Decapsulation • Configure TCP Tunnel

Create GigaSMART Operations – A Summary

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

GigaSMART operations require the following steps:

1. **Create GigaSMART groups on the GigaSMART Groups page (select GigaSMART > GigaSMART Groups > GigaSMART Groups)**

Use GigaSMART groups to manage and budget GigaSMART processing power. Use the **New** button on the GigaSMART Group page to create groups of the available GigaSMART ports in a given chassis.

NOTE: The GigaSMART engine ports in a GigaSMART group can be on different line cards or modules in the same GigaVUE-HC3 chassis. However, all GigaSMART engine ports must be on the same chassis.

The number of GigaSMART engine ports are as follows:

- The GigaSMART-HC0 module includes one GigaSMART engine port.
- The GigaVUE-HC1 node includes one GigaSMART engine port.

The number of GigaSMART engine ports available in a chassis depends on the number of GigaSMART line cards in the chassis

The processing power of the GigaSMART engine ports is as follows:

- Each GigaSMART port on the GigaSMART-HC0 module can process packets at **40Gb**.
- GigaSMART port on the GigaVUE-HC1 node can process packets at **20Gb**.

GigaSMART engine ports are numbered with an **e** prefix using **<bid/sid/e1..e2>** nomenclature – **1/1/e1**, for example.

NOTE: The ports in a GigaSMART group can be on different line cards or modules in the same GigaVUE-HC3 chassis. However, they must all be on the same chassis.

NOTE: The slot ID for a GigaVUE-HC1 chassis is fixed at **1**.

Each GigaSMART operation you create in the next step must be assigned to one of the GigaSMART groups you create in this step. You can select GigaSMARToperation only when the card supports the operation.

2. Create GigaSMART operations using the GigaSMART Operations page (select **GigaSMART > GigaSMART Operations (GSOP)**)

Give your GigaSMART operation a name, include a valid combination of GigaSMART operations, and assign it to one of the GigaSMART groups created in the previous step.

Refer to [How to Combine GigaSMART Operations](#) for details on supported combinations of GigaSMART operations.

You can also configure how (or, in some cases, whether) a GigaSMART operation attaches a trailer that indicates where a packet arrived in the Gigamon Deep Observability Pipeline and how it was modified. This trailer can be interpreted using a recent version of the Wireshark® Protocol Analyzer. Refer to [GigaSMART Trailer Reference](#) for details on the GigaSMART Trailer.

3. Apply GigaSMART operations to network ports in maps

The New Map and Edit Map pages contain a **GigaSMART Operations (GSOP)** field that lets you select a GigaSMART operation to be used in a map. Refer to [Manage Maps](#) for details. Keep in mind, however, that GigaSMART operations **must** be selected before destination tool ports or collector destinations.

Groups of GigaSMART Engine Ports

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

Use the GigaSMART Group page to create groups of GigaSMART engine ports in a given GigaSMART chassis. (To go to the GigaSMART Group page, select **GigaSMART > GigaSMART Groups > GigaSMART Groups > New.**)

NOTE: You cannot create a new group of GigaSMART engine ports when no GigaSMART engine ports are available on the device.

The GigaSMART engine ports in a GigaSMART group can be on different line cards or modules in the same GigaVUE-HC3 chassis. However, all GigaSMART engine ports must be on the same chassis.

Use groups of GigaSMART engine ports to increase the processing power of GigaSMART. The processing power of the GigaSMART engine ports is as follows:

- Each of the two GigaSMART engine ports in an SMT-HC3-C05 module on GigaVUE-HC3 can process packets at up to **100Gb**.
- Each of the two GigaSMART engine ports in an SMT-HC3-C08 module on GigaVUE-HC3 can process packets at up to **200Gb**.
- The GigaSMART engine port in the GigaVUE-HC1 node can process packets at up to **20Gb**.
- The GigaSMART engine port in the GigaVUE-HC1 Gen3 can process packets at up to **80Gb**.
- The GigaSMART engine port in the GigaVUE-HC1-Plus node can process packets at up to **100Gb**.
- The GigaSMART engine port in the GigaVUE-HCT Gen3 can process packets at up to **80Gb**.

The number of GigaSMART engine ports are as follows:

- Each GigaSMART-HC0 module includes one GigaSMART engine port.
- Each SMT-HC3-C05 module on GigaVUE-HC3 includes two GigaSMART engine ports.
- The GigaVUE-HC1 node includes one GigaSMART engine port.
- The GigaVUE-HC1-Plus node includes one fixed GigaSMART module.

The number of GigaSMART engine ports available in a chassis depends on the number of GigaSMART line cards or modules in the chassis as follows:

- Up to four modules in the GigaVUE-HC3 (eight GigaSMART engine ports).
- One module in GigaVUE-HC1 (one engine port).
- Up to two modules in GigaVUE-HC1 Gen 3 (two GigaSMART engine ports).
- One module in GigaVUE-HCT Gen3 (one engine port).

The following table provides a summary:

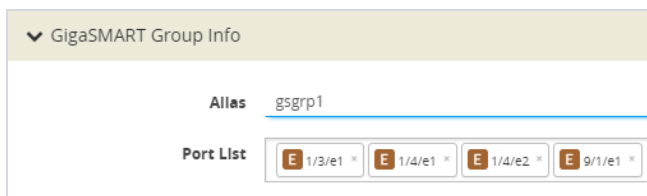
GigaSMART Node	Maximum GigaSMART Line Cards or Modules per Node	Number of GigaSMART engine ports per Line Card or Module	Maximum Number of GigaSMART engine ports in a GigaSMART group (gsgroup)
GigaVUE-HC3	4	2	8
GigaVUE-HC1	1 built-in	1	1
GigaVUE-HC1 Gen3	2	1	2
GigaVUE-HC1-Plus	1 built-in rear module, 1	2	2
GigaVUE-HCT Gen3	1 built-in front	1	1

NOTE: Grouping Generation 3 and Generation 2 cards is not supported.

NOTE: On supported GigaVUE HC Series platforms with Generation 3 GigaSMART cards, you can use the GigaSMART Groups page to reload one or more GigaSMART engine ports in a group. This provides a granular way to reset only the engines in a selected group without reloading the entire chassis or GigaSMART card. Reload is not available on Generation 2 cards or on GigaSMART Appliance (GSA).

Engine grouping for GTP is a special case, which is described in [GTP Engine Grouping](#).

GigaSMART engine ports are numbered with an **e** prefix using **<bid/sid/e1..e2>** nomenclature, such as 1/1/e1. For example:



Reload GigaSMART engine ports in a group

On supported GigaVUE HC Series devices with Generation 3 GigaSMART cards, you can reload one or more GigaSMART engine ports in an existing GigaSMART group. Reloading a group restarts the selected engines in that group without rebooting the chassis or the GigaSMART card.

Use this operation to recover or troubleshoot a group while minimizing impact to other traffic.

To reload GigaSMART engine ports in a group:

1. In GigaVUE-FM, navigate to the device and select **GigaSMART > GigaSMART Groups**.
2. On the GigaSMART Groups page, select the GigaSMART group (gsgroup) that you want to reload.
3. From the **Actions** menu, choose **Reload**.
4. In the reload dialog:
 - Review the list of GigaSMART engine ports that belong to the selected group.
 - By default, all ports are selected.
 - To minimize impact, clear any engine ports that you do not want to reload so that only the affected engines are reloaded.

5. If the group is configured for an Inline traffic then a is displayed, review the warning that reload will impact traffic on that group and proceed only if you have planned for a brief disruption.
6. Click ****Apply**** to start the reload.

Only the selected GigaSMART engine ports in the group are reloaded; other groups and unrelated traffic on the device continue to run. The reload is a software-level restart of the engines and does not reboot the chassis or the GigaSMART card.

How to Use GigaSMART Operations – Example

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

The following procedure summarizes the major steps in creating and using a GigaSMART operation.

1. From the device view, start by selecting **GigaSMART > GigaSMART Groups > GigaSMART Groups** and clicking **New** to create a **GigaSMART group** – a collection of one or more internal GigaSMART ports available in a given chassis. GigaSMART groups are used to process GigaSMART operations – each GSOP you create is assigned to a GigaSMART group.

In this example, a GigaSMART group called **GS1** is created that uses virtual port **e1** on the GigaSMART-HD0 line card in slot 2 of box 16 (**16/2/e1**):

On the GigaSMART Group configuration page:

- a. Enter GS1 in the **Alias** field.
- b. Click in the **Port List** field to select the port.

On the GigaSMART Group configuration page, you can also set parameters for specific types of GigaSMART operations.

- c. Click **Save**.

2. Next, you can create a **GigaSMART operation** – a combination of packet modification actions that can be used in a map – and assign it to a GigaSMART group for processing.

In this example, a GigaSMART operation called **tcpmask** is created that will overwrite 16 bytes of packet data starting 64 bytes after the end of the TCP header using a hexadecimal **ee** pattern. The GigaSMART operation is assigned to the **GS1** GigaSMART group created in the first step.

To create a GigaSMART operation called **tcpmask**:

- a. From the device view, select **GigaSMART > GigaSMART Operations**, and then click **New**.
- b. In the **Alias** field, enter **tcpmask**.
- c. Click in the **GigaSMART Groups** field and select **GS1** from the list of GigaSMART groups.
- d. Click in the **GigaSMART Operations (GSOP)** field and select **Masking** from the list. The configuration dialog for Masking displays.
- e. Configure Masking as follows:
 - **Protocol**: TCP
 - **Offset**: 64
 - **Pattern**: ee
 - **Length**: 16

3. Once you have set up a GigaSMART operation, you can include it as part of a map with the **GigaSMART Operations (GSOP)** field in the Map configuration page. In this example, the **tcpmask** GigaSMART operation is combined with an IP Version pass rule so that all IPv4 traffic processed is masked according to the GSOP created in the previous step.

If you are not sure which GigaSMART operation you want to use, click in the GSOP field to display a list of the operations you have already configured.

To configure the map:

- a. Select **Maps > Maps > Maps**, and then click **New** to open the New Map page.
- b. On the New Map page, configure the map as follows:
 - **Alias**: gsmmap
 - **Type**: Regular
 - **Subtype**: By Rule
 - **Source**: select the network ports (for example: 16/3/x7, 16/3/x8, 16/3/x9, 16/3/x10, 16/3/x11, 16/3/x12)
 - **Destination**: select the tool port (for example: 16/3/x1)
 - **GigaSMART Operations (GSOP)**: tcpmasking (GS1)
- c. Click **Add Rule** and specify the following for the rule:
 - Select **Pass**
 - Click in the **Rule** field and select **IP Version**
 - Select **v4** for **Version**.
- d. Click **Save**.

Here, a map named **gsmap** is created that forwards IPv4 traffic from network ports 16/3/x7..x12 to tool port 16/3/x1. The traffic will be masked using the **tcpmask** GigaSMART operation created in Step 2.

Engine Watchdog Timer in GigaSMART

In rare scenarios, a packet processing core in the CPU of a GigaSMART engine can enter a deadlocked state. The engine watchdog timer detects the issue and reloads the GigaSMART engine after a specified number of seconds. The engine watchdog timer is enabled by default with a value of 60 seconds. The maximum number of seconds is 600 seconds.

NOTE: If a core is in a deadlocked state, all packets are dropped.

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

To configure the engine watchdog timer, do the following:

1. From the device view, select **GigaSMART > GigaSMART Groups > GigaSMART Groups**.
2. Click **New**.

NOTE: If you are modifying an existing GigaSMART Group, select the GS Group and click **Edit**. Otherwise, .

3. In the **Alias** field, enter an alias for this GS Group.
4. In **Port List** field, select the engine port for this GS Group.
5. Under **Engine Timer**, do the following:
 - a. Select **Enable** to enable the time or clear the checkbox to disable the timer.
 - b. In the **Engine Watchdog Time field**, set the number of seconds to wait before reloading the engine. The minimum is 60. The maximum is 600.

In the following example, the timer is enabled and set to 100 seconds.

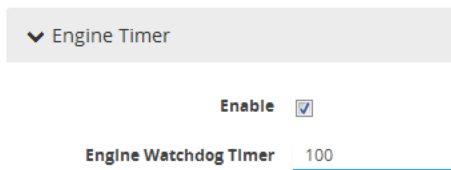


Figure 1 Engine Watchdog Timer

Tunnel Health Checks

Starting in software version 5.3, there are tunnel health checks. The reachability of IP destinations is checked and, if the destinations are not reachable, packets will not be sent or will stop being sent.

The tunnel health check on the GigaSMART card defines destinations as follows:

- IP destinations used for sending packets from a single IP interface with tool port to a single IP destination
- tunnel endpoints used for load balancing from a single IP interface with tool port to multiple IP destinations

An SNMP notification can be sent when the status of a IP destination or tunnel endpoint changes, either from Up to Down or from Down to Up.

NOTE: Tunnel Health-check is not supported for GMIP tunnel.

To enable the SNMP notification, refer to [Enable or Disable Events for SNMP Notifications](#).

To configure ICMP health check parameters for the GigaSMART group, refer to [Figure 2Configure ICMP Health Check Parameters](#).

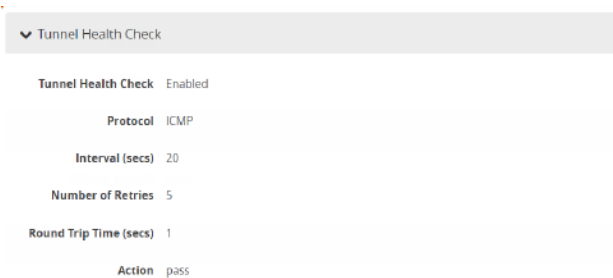


Figure 2 Configure ICMP Health Check Parameters

To configure UDP health check parameters for the GigaSMART group, refer to [Figure 3Configure UDP Health Check Parameters](#).

▼ Tunnel Health Check

Tunnel Health Check

Enabled

Protocol

UDP

Source Port

54321

Destination Port

54321

Receive Port

54321

Interval (secs)

20

Number of Retries

5

Round Trip Time (secs)

1

Action

pass

Figure 3 Configure UDP Health Check Parameters

To view IP interface status, refer to [Figure 4View IP Destination Status](#).

☐	Alias	Port	Status	Type	IP Address	IP Mask	Gateway	MTU	Hardware Address	GS Groups	Exporters	Comment
☐	giga_auto_tunn...	3/4/x12	Port is Healthy	IPv4	10.115.32.98	255.255.248.0	10.115.32.1	1500	00:1D:AC:7C:06:47	1 GS Group		Auto generated IP interface for...
☐	giga_auto_tunn...	3/4/x14	Port is Healthy	IPv4	10.115.32.195	255.255.248.0	10.115.32.1	1500	00:1D:AC:7C:06:49	1 GS Group		Auto generated IP interface for...
☐	giga_auto_tunn...	3/4/x13	Port is Healthy	IPv4	10.115.32.194	255.255.248.0	10.115.32.1	1500	00:1D:AC:7C:06:48	1 GS Group		Auto generated IP interface for...
☐	giga_auto_tunn...	3/4/x16	Port is Healthy	IPv4	10.115.32.193	255.255.248.0	10.115.32.1	1500	00:1D:AC:7C:06:4B	1 GS Group		Auto generated IP interface for...
☐	giga_auto_tunn...	3/4/x15	Component(s) cluster_gs_group ports are ...	IPv4	10.115.32.197	255.255.248.0	10.115.32.1	1500	00:1D:AC:7C:06:4A	1 GS Group		Auto generated IP interface for...

Figure 4 View IP Destination Status

To view tunnel endpoint status, refer to [Figure 5View Tunnel Endpoint Status](#).

☐	↑ Tunnel Endpoint ID	Alias	IP Address	Status
☐	te1		192.168.1.145	Up
☐	te2		192.168.1.188	Down
☐	te3		192.168.1.123	Up
Total Items : 3				

Figure 5 View Tunnel Endpoint Status

To view IP interface statistics, refer to [Figure 6View IP DestinationStatistics](#).

IP Interface	Bytes Rx	Bytes Tx	Packets Rx	Packets Tx	Multicast Packets Rx	Discards Rx	Discards Tx	Errors Rx	Errors Tx	Overruns Rx	Overruns Tx	Frame Rx	Carrier Tx	Collisions Tx
giga_auto_tunn...	109266444	176576	1707260	2759	0	0	0	0	0	0	0	0	0	0
giga_auto_tunn...	109266380	176576	1707259	2759	0	0	0	0	0	0	0	0	0	0
giga_auto_tunn...	0	640	0	10	0	0	0	0	0	0	0	0	0	0
giga_auto_tunn...	109272652	176640	1707357	2760	0	0	0	0	0	0	0	0	0	0
giga_auto_tunn...	109266636	176512	1707263	2758	0	0	0	0	0	0	0	0	0	0

Figure 6 View IP DestinationStatistics

To view GigaSMART operation statistics, refer to [Figure 7View GigaSMART Operation Statistics](#).

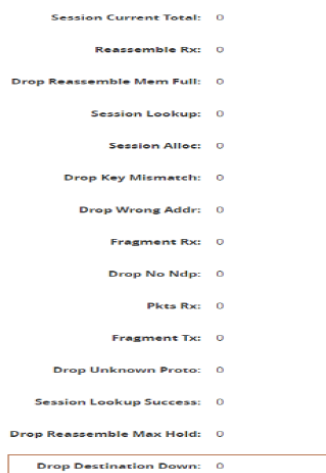


Figure 7 View GigaSMART Operation Statistics

Configure Hashing

The **Hash** option in the GigaSMART Group page allows you to select the required hashing option for the GigaSMART Groups. The following options are available:

- **Advanced:** Advanced hashing. Refer to the “*Fabric Advanced Hashing*” section in the *GigaVUE Administration Guide*.
- **IPSrcIPDst:** Fixed two tuple hashing based on outer IP, Src and Dst.

GigaSMART Rules and Tips

When using GigaSMART operations, keep in mind the following rules and tips:

Note	Description
Use on Any GigaSMART-Enabled Node	Maps including GigaSMART operations can be bound to any network port on a GigaSMART-enabled node: - o Standalone GigaVUE-HC3 with SMT-HC3-C05 module. - o Standalone GigaVUE-HC1 nodes. - o Any GigaSMART H Series node operating in a cluster with one of these node types. Clustered nodes can use maps with GigaSMART operations so long as there is at least one node available in the cluster with GigaSMART capabilities. The GigaSMART group used to power the GigaSMART operation does not need to reside on the same physical chassis as the network or tool ports for the map. Refer to GigaSMART Operations in Clusters for some illustrations of how this

Note	Description
	works.
Use in Maps with Standard Rule Criteria	Combine GSOPs with map rules carefully to ensure selective application. For example, headers in an IPv4 packet end at a different offset than those in an IPv6 traffic. You can create maps for the following: - o Identify IPv4 traffic, slice it at a 64-byte offset and forward the results to tool port 5. - o Identify IPv6 traffic, slice it at an 82-byte offset and forward the results to tool port 6. GSOPs are applied to all packets matching any rule in the map in which the GSOP is included.
Editing Maps and GSOPs	Maps containing GigaSMART operations (GSOPs) should not be edited. Also GSOPs should not be edited once they are associated with maps. Note: In Gen3 platform, if there are multiple maps with GSOPs sourcing from the same network ports, when you edit, delete, or reconfigure a map, traffic drop from one map to another maps GSOP will be observed.
Rules for Tunneling Operations	The rules for tunneling operations are as follows: - o A map including a GigaSMART operation with a tunnel decapsulation component (tunnel-decap) cannot also include a collector rule. The system prevents situations that would violate this rule. - o GigaSMART operations with a tunnel decapsulation component can only be assigned to GigaSMART groups consisting of a single GigaSMART port. - o IP interfaces cannot be shared with map-passalls, tool-mirrors, port-pairs, or other regular maps. - o For devices involved in tunneling using GMIP. the recommendation is that they run the same software version on both sides of the tunnel (encapsulating/decapsulating).
Combine Multiple Components in a Single Operation	You can combine multiple GigaSMART components into a single operation. For example, you could set up a single GigaSMART operation that masks a packet, strips its VLAN header, and applies a trailer. Note: With the exception of slicing and masking, most GigaSMART components can be combined in a single operation. Slicing and masking can be combined with other components but not with each other. Refer to How to Combine GigaSMART Operations for details on the combinations of GigaSMART operations. Note: The [trailer <remove>] argument cannot combined with others – it must be used by itself. Refer to Remove GigaSMART Trailers for details. Note: NetFlow can only be combined with de-duplication and with APF (using second level maps).
GigaVUE-HC3 Nodes with Multiple GigaSMART Modules	The GigaVUE-HC3 chassis supports up to four GigaSMART SMT-HC3-C05 modules. Each module has two GigaSMART engine ports. Each GigaSMART engine port can process packets at up to 100Gb.

Virtual Ports

Virtual ports (vports) are used in flow maps to aggregate and redirect traffic to the GigaSMART ports. It is an aggregation point for traffic to be directed to the GigaSMART second level maps. Second level maps are used for configuring filtering rules enabled through GTP correlation and Adaptive Packet Filtering (APF).

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

Virtual Port Rules

The following rules apply to single virtual ports:

1. A given vport can only belong to one GigaSMART group.
2. Different first level maps with the same network ports can use the same vport. However, you must keep in mind the limitation described in Rule 1.
3. Different first level maps with different network ports can use the same vport. However, you must keep in mind the case described in Rule 2.
4. Different vports can be configured on the same GigaSMART group, but must be used in different maps.
5. A GigaSMART operation can only belong to one GigaSMART engine group.
6. In a first level map, you can specify a vport but not a GigaSMART operation.
7. The vport and the GigaSMART operation used in a second level map must be defined on the same GigaSMART group.
8. In a second level map, a maximum of 5 maps are allowed to be attached to a vport. The maximum number of gsrules in each map is 5. The maximum number of flowrules in each map is 32.
9. Multiple GTP flow sampling maps can receive traffic from the same virtual port when **GTP Overlap** is enabled.

Create Virtual Port

To create a virtual port, use the following procedure:

1. From the device view, select **GigaSMART > Virtual Ports**.
2. Click **New**.
3. On the Virtual Ports page, do the following:
 - a. In the **Alias** field, enter a name for the virtual port. For example, gsTraffic.
 - b. From the GigaSMART Group drop-down list, select the GigaSMART group to associate with the virtual port. For example, gsgrp1.
 - c. Select the GTP Overlap check box to enable multiple GTP flow sampling maps to receive traffic from the same virtual port.
 - d. In the Inline Failover Action drop-down list, select one of the following options:
 - **Tool Bypass** — When the inline tool fails, all traffic coming to the respective inline tool is directed via the bypass path.
 - **Network Bypass** — When the inline tool fails, the traffic is directed to multiple inline tools associated with an inline network or inline network group using rule-based inline maps.
 - **Tool Drop** — When the inline tool fails, all traffic coming to the respective inline tool is dropped.
 - **Network Drop**—When the inline tool fails, all traffic coming to the respective inline tool is dropped.
 - **Network Port Forced Down**—When the inline tool fails, the inline network ports of the respective inline network are forced as "down".
 - e. Click **OK**.
4. Create a GigaSMART operation with an Adaptive Packet Filtering (APF) component.
 - a. From the device view, select **GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation**.
 - b. Click **New**.
 - c. In the **Alias** field, enter g1 for the GigaSMART Operation.
 - d. From the **GigaSMART Groups** list, select a GigaSMART group.
 - e. From the GigaSMART Operations (GSOP) list, select **Adaptive Packet Filtering**.
5. Create a first-level map name map1 to direct traffic to the virtual port gsTraffic.
 - a. Go to the Maps page and click **New**. The New Map page opens.
 - b. Enter map1 in the **Alias** field.
 - c. For **Type**, select **First Level** and for **Subtype** select **By Rule** map
 - d. For **Source**, select a network port. For example, a network port with the alias N1.
 - e. For **Destination**, select the virtual port (gsTraffic).
 - f. Click Add a Rule, and create rule with the following conditions:

- Pass
- VLAN 20
- IPv4 Protocol UDP
- Port Destination 2152

g. Click **Save**.

6. Create second-level maps named map2 and map3 to direct traffic from the virtual port to the GigaSMART operation.

Configure the map map2 with the **Source** as virtual port gsTraffic, the **Destination** as port T1, and select g1 for **GigaSMART Operation (GSOP)**. For map2, add the following two rules.

Rule 1:

- Pass
- IPv4 Destination 65.128.7.21 Cidr 32
- IPv4 Protocol TCP
- Port Destination 80

Rule 2:

- Pass
- IPv4 Destination 98.43.132.70 Cidr 32
- IPv4 Protocol TCP
- Port Destination 80

Configure the map map3 with the **Source** as virtual port gsTraffic, the destination **Destination** as port T2, and g1 for **GigaSMART Operation (GSOP)**. For map3, add the following two rules.

Rule 1:

- Pass
- IPv4 Destination 65.128.7.21 Cidr 32
- IPv4 Protocol TCP
- Port Destination 443

Rule 2:

- Pass
- IPv4 Destination 98.43.132.70 Cidr 32
- IPv4 Protocol TCP
- Port Destination 443

If there are other GigaSMART applications defined in the GigaSMART operation, filtering will be done on the packets before sending the GigaSMART applications.

7. Create a shared collector map name mapC1 to direct traffic not matching the second-level maps to the tool port with the alias T3. The collector for the first-level map named map1 uses the standard collector available in prior releases.

- a. Go the Maps page and click **New**. The New Page page opens.
- b. In the **Alias** field, enter mapC1.
- c. For **Type**, select **Regular**.
- d. For **Subtype**, select **Collector**.
- e. For **Source**, select the virtual port gsTraffic.
- f. For **Destination**, select the tool port with the alias T3, and the click **Save**.

Task	Navigation Path
Clone the configurations of an existing virtual port	In the device view select GigaSMART > Virtual Ports > Actions > Clone
Edit an existing virtual port	In the device view select GigaSMART > Virtual Ports > Actions > Edit
Delete a virtual port	In the device view select GigaSMART > Virtual Ports > Actions > Delete

Multiple Virtual Ports for First Level Map

A first level map can have multiple virtual ports (vports). When multiple vports are configured on a first level map, data is sent from network ports to the multiple vports destined to specific GigaSMART groups.

The tool ports of a first level map can be a combination of vports and tool ports. Each vport is bound to a GigaSMART group (gsgroup). Multiple vports are bound to multiple gsgroups. However, in a single first level map, all the vports must be bound to different gsgroups.

NOTE: For a second level map, only a single vport can be configured.

When a second level map is configured using a vport, the data that is sent to the gsgroup is forwarded to the tool ports according to the gsrules or flow rules configured on the map.

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

To configure multiple vports for a first level map:

1. Create gsgroups on the GigaSMART engine, using the following steps to create a gsgroup with the alias gsgroup1 and one with the alias gsgroup2:
 - a. From the device view, select **GigaSMART > GigaSMART Groups > GigaSMART Groups**.
 - b. Click **New**.
 - c. Enter an alias for the GigaSMART Group in the **Alias** field.
 - d. Click in the **Port List** field to select an engine port.
 - e. Enable parameters on the GigaSMART Group as needed. For example, to enable GTP correlation, enter the Timeout value under **GTP Flow**.
 - f. Click **Save**.
 - g. Repeat steps b through f to add another GigaSMART Group.
2. Enable GTP correlation on the GigaSMART groups.
 - a. From the device view, select **GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation**.
 - b. Click **New**.
 - c. Enter a name for the GigaSMART Operation in the **Alias** field (for example gsl).
 - d. Select the GigaSMART groups from the **GigaSMART Groups** list.
 - e. Select **Flow Filtering** from the GigaSMART Operations (GSOP) list.
 - f. Click **Save**.
 - g. Repeat steps a through f to create the second GigaSMART Operation.

3. Create vports (for example, vp1 and vp2) and assign them to the gsgroups. For the steps to create a virtual ports, refer to [Virtual Ports](#).
1. Create a **First Level By Rule** map and direct traffic to both vports and a tool port by navigating to the Maps page and clicking **New**.
 - a. Enter a name for the map in the **Alias** field. For example, map1.
 - b. Select **First Level** for **Type** and **By Rule** for **Subtype**.
 - c. Specify networks ports in the **Source** field.
 - d. Select the virtual ports and a tool port in the **Destination** field.
 - e. Click **Add Rule**.
 - f. Select **Pass** and **Port Destination** for ports 251 to 252.
 - g. Click **Save**.
4. Create a second level map named to direct traffic from the first vport (vp1) to the GTP correlation GigaSMART operation by navigate to the Maps page and clicking **New**.
 - a. Enter a name for the map in the **Alias** field. For example, map2.
 - b. Select **Second Level** for **Type** and **Flow Filtering** for **Subtype**.
 - c. Specify the first virtual port (vp1) in the **Source** field.
 - d. Select a tool port in the **Destination** field.
 - e. Click in the **GigaSMART Operation (GSOP)** field and select GSOP from the list. For example, gs1.
 - f. Click **Add Rule**.
 - g. Select **Pass** and **GTP IMSI**.
 - h. Enter 302720* in the IMSI field and select **Version V1**.
 - i. Click **Save**.
5. Create a shared collector map to direct traffic not matching the second level map to a tool port by navigating to the Maps page and clicking **New**.
 - a. Enter a name for the map in the **Alias** field. For example, sc1.
 - b. Select **Second Level** for **Type** and **Collector** for **Subtype**.
 - c. Select the first virtual port (vp1) in the **Source** field.
 - d. Select a tool port in the **Destination** field.

6. Create a second level map named **map3** to direct traffic from the second vport (vp2) to the GTP correlation GigaSMART operation by navigating to the Maps page and clicking **New**.
 - a. Enter a name for the map in the **Alias** field. For example, map3.
 - b. Select **Second Level** for **Type** and **Flow Filtering** for **Subtype**.
 - c. Specify the second virtual port (vp2) in the **Source** field.
 - d. Select a tool port in the **Destination** field.
 - e. Click in the **GigaSMART Operation (GSOP)** field and select GSOP from the list. For example, gs2.
 - f. Click **Add Rule**.
 - g. Select **Pass** and **GTP IMSI**.
 - h. Enter * in the IMSI field.
 - i. Click **Save**.

Multiple Virtual Port Rules

The following rules apply to multiple virtual ports for first level maps:

1. Multiple vports with different GigaSMART groups (gsgroups) can be used on a first level map.
2. Different vports can be configured on the same GigaSMART group, but must be used in different maps.
3. A gsgroup can have multiple GigaSMART operations (gsops).
4. Only one vport is allowed on egress (second level) maps.
5. A vport on a first level map cannot be edited. To make a map change, delete the vport from the **Destination** field first and then add a new vport by clicking in the **Destination** field and selecting another vport.
6. In a standalone system, the number of vports for a first level map is limited by the number of GigaSMART engines (eports) in the chassis.
7. In a cluster environment, the number of vports for a first level map is limited by the number of eports in the cluster.

Multiple Virtual Port with Other GigaSMART Applications

The example in [Multiple Virtual Ports for First Level Map](#) uses the GTP correlation GigaSMART operation. You can also use multiple vports with other GigaSMART operations, such as Adaptive Packet Filtering (APF). You can also chain multiple GigaSMART applications. This allows you to perform different functions and filtering with the same packets.

To access GigaSMART within GigaVUE-FM, access a device that has been added to GigaVUE-FM from the GigaVUE-FM interface. GigaSMART appears in the navigation pane of the device view on supported devices. Refer to [Access GigaSMART from GigaVUE-FM](#) for details.

To configure multiple vports for a first level map:

1. Create GigaSMART Groups on the GigaSMART engines, using the following steps to create three gsgroups with the aliases gg2, gg3, and gg5 and associate with gsops gs2, gs3, and gs5, respectively.
 - a. From the device view, select **GigaSMART > GigaSMART Groups > GigaSMART Groups**.
 - b. Click **New**.
 - c. Enter an alias for the GigaSMART Group in the **Alias** field. (In this example, gg2, gg3, or gg5.)
 - d. Click in the **Port List** field to select an engine port.
 - e. Enable parameters on the GigaSMART Group as needed. For example, to enable GTP correlation, enter the Timeout value under **GTP Flow**.
 - f. Click **Save**.
 - g. Repeat steps b through f to add another GigaSMART Group.
2. Enable APF on the GigaSMART groups, using the following steps:
 - a. From the device view, select **GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation**.
 - b. Click **New**.
 - c. Enter an alias for the GigaSMART Operation in the **Alias** field. (In this example, gs2, gs3, or gs5.)

- d. Select the GigaSMART group from the **GigaSMART Groups** list. (For gs2, select gg2. For gs3, select gg3. For gs5, select gg3.)
 - e. Select **APF** from the GigaSMART Operations (GSOP) list and select **Enable**.
 - f. Select **Slicing** from the GigaSMART Operations (GSOP) list, and then set **Protocol** to none. For gs2 set the **offset** to 80. For gs3, set the **offset** to 90. For gs5, set the **offset** to 100.
 - g. Click **Save**.
 - h. Repeat steps a through f to create another GigaSMART Operation.
3. Create vports and assign them to the GigaSMART Groups, using the following steps to create three virtual ports named vp2, vp3, and vp4, assigning them to gsgroup gg2, gg3, and gg5 respectively.
 - a. From the device view, select **GigaSMART > Virtual Ports**.
 - b. Click **New**.
 - c. Enter an alias for the virtual in the **Alias** field. (In this example, vp2, vp3, or vp5.)
 - d. Select the gsgroup from the **GigaSMART Group** field (gg2 for vp2, gg3 for vp2, and gg5 for vp5).
 - e. Click **Save**.
 - f. Repeat step b through step e to create another virtual port.
4. Create a first level map, and direct traffic to two vports and a tool port, using the following steps:
 - a. Select **Maps > Maps > Maps**.
 - b. Click **New**.
 - c. Enter m1 in the **Alias** field.
 - d. Select **First Level** for **Type** and **By Rule** for **Subtype**.
 - e. Select a network port in the **Source** field.
 - f. Select virtual ports vp2 and vp3 plus a tool port in the **Destination** field.
 - g. Use the **Add a Rule** button to add two rules to the map.

For the first rule, select **pass** and select **VLAN** for the condition. Set the VLAN value to 100.

For the second rule, select **pass** and select **VLAN** for the condition. Set the VLAN value to 200.
 - h. Click **Save**.

5. Create a second level map named to direct traffic from the vports to the GigaSMART operation, using the following steps:
 - a. Select **Maps > Maps > Maps**.
 - b. Click **New**.
 - c. Enter m2 in the **Alias** field.
 - d. Select **Second Level** for **Type** and **By Rule** for **Subtype**.
 - e. Select a virtual port vp2 the **Source** field.
 - f. Select a tool port in the **Destination** field.
 - g. Select gs2 for **GigaSMART Operation (GSOP)**.
 - h. Use the **Add a Rule** button to add a rules to the map.

For the rule, select **pass** and select **VLAN** for the condition. Set the VLAN value to 100 with **Subset** set to none and **Position** set to 0.
 - i. Click **Save**.
6. Create another second level map named to direct traffic from the vports to the GigaSMART operation, using the following steps:
 - a. Select **Maps > Maps > Maps**.
 - b. Click **New**.
 - c. Enter m4 in the **Alias** field.
 - d. Select **Second Level** for **Type** and **By Rule** for **Subtype**.
 - e. Select a virtual port vp3 in the **Source** field.
 - f. Select a tool port in the **Destination** field.
 - g. Select gs3 for **GigaSMART Operation (GSOP)**.
 - h. Use the **Add a Rule** button to add a rules to the map.

For the rule, select **pass** and select **VLAN** for the condition. Set the VLAN value to 200 with **Subset** set to none and **Position** set to 0.
 - i. Click **Save**.
7. Create another second level map to direct traffic from the vports to the GigaSMART operation.
 - a. Select **Maps > Maps > Maps**.
 - b. Click **New**.
 - c. Enter m6 in the **Alias** field.
 - d. Select **Second Level** for **Type** and **By Rule** for **Subtype**.

- e. Select a virtual port vp3 in the **Source** field.
 - f. Select a tool port in the **Destination** field.
 - g. Select gs3 for **GigaSMART Operation (GSOP)**.
 - h. Use the **Add a Rule** button to add a rules to the map.
For the rule, select **pass** and select **VLAN** for the condition. Set the VLAN value to 200 with **Subset** set to none and **Position** set to 0.
 - i. Click **Save**.
8. Create a shared collector map named to direct traffic not matching the maps to a tool port.
- a. Select **Maps > Maps > Maps**.
 - b. Click **New**.
 - c. Enter sc1 in the **Alias** field.
 - d. Select **Second Level** for **Type** and **Collector** for **Subtype**.
 - e. Select a virtual port vp1 in the **Source** field.
 - f. Select a tool port in the **Destination** field.
 - g. Click **Save**.

Virtual Port Statistics

The Virtual Ports page displays statistics about the configured virtual ports. To view the statistics select **GigaSMART > Virtual Ports > Statistics**.

The following table describes virtual port statistics:

Statistic	Description
Rx Packets	The number of packets received into the virtual port.
Tx Packets	The number of packets transmitted out of the virtual port.
Rx Octets	The number of bytes received into the virtual port.
Tx Octets	The number of bytes transmitted out of the virtual port.
Packets Drops	The number of packets dropped at the virtual port.
Packet Drops No Init	For internal debugging.

Differences in GigaSMART Nomenclature Between the CLI and GigaVUE-FM

The CLI and the Web-based GigaVUE-FM interface occasionally use different names to refer to the same GigaSMART-related functionality. The following table summarizes the differences:

Documentation Term	CLI Term	GigaVUE-FM Term	Description
GigaSMART Port	e1, e2	GigaSMART Engine	Internal ports on GigaSMART line card, module used to power GigaSMART features.
GigaSMART Group	gsgroup	GigaSMART Engine Group	Group of internal ports on GigaSMART line card, module used to power GigaSMART features. You configure these in the CLI with the gsgroup command.
GigaSMART Component	gsop	GigaSMART Operation	One of the available GigaSMART packet processing features (de-duplication, slicing, and so on)
GigaSMART Operation	gsop	GigaSMART Operation Group	A combination of GigaSMART packet-processing features into a single entity used in a map. You configure these in the CLI with the gsop command.

GigaSMART Operations in Clusters

Clustered environments with at least one GigaSMART-enabled chassis can take advantage of GigaSMART operations in maps on network ports elsewhere in the cluster. As shown in [Figure 8 GigaSMART Group on Different Chassis than Network/Tool Ports](#) and [Figure 9 GigaSMART Operations in Clusters](#), the GigaSMART group providing the packet processing power for a GigaSMART operation does not have to be on the same chassis as the network or tool ports for a map.

- A map's network ports, tool ports, and the GigaSMART group ports can all be on different nodes in a clustered environment.
- GigaSMART operations do not require any specific role for the chassis with the GigaSMART group – it can be a leader, standby, or normal node.
- The main requirements to keep in mind is that the GigaSMART ports in a GigaSMART group must all be on the same chassis. So, for example, if you had two GigaSMART-HD0 line cards in a single chassis, you could create a single GigaSMART

group out of the four GigaSMART engine ports available across the two line cards. However, if the two line cards were in two different chassis, they could not be combined into a single GigaSMART group.

NOTE: Inline SSL is not supported in clusters nor on any nodes that are part of a cluster. Do not attempt to enable inline SSL on individual nodes that are part of a cluster or have inline networks and inline tools distributed among various nodes in a cluster.

Figure 8 [GigaSMART Group on Different Chassis than Network/Tool Ports](#) and Figure 9 [GigaSMART Operations in Clusters](#) illustrate examples of network, tool, and GigaSMART group ports on different nodes in a clustered environment. For example, Figure 8 [GigaSMART Group on Different Chassis than Network/Tool Ports](#) shows a map accepting ingress packets on GV1, sending them to the GigaSMART group on GV3 for GigaSMART processing (for example, de-duplication), and sending the results to a tool port on GV4.

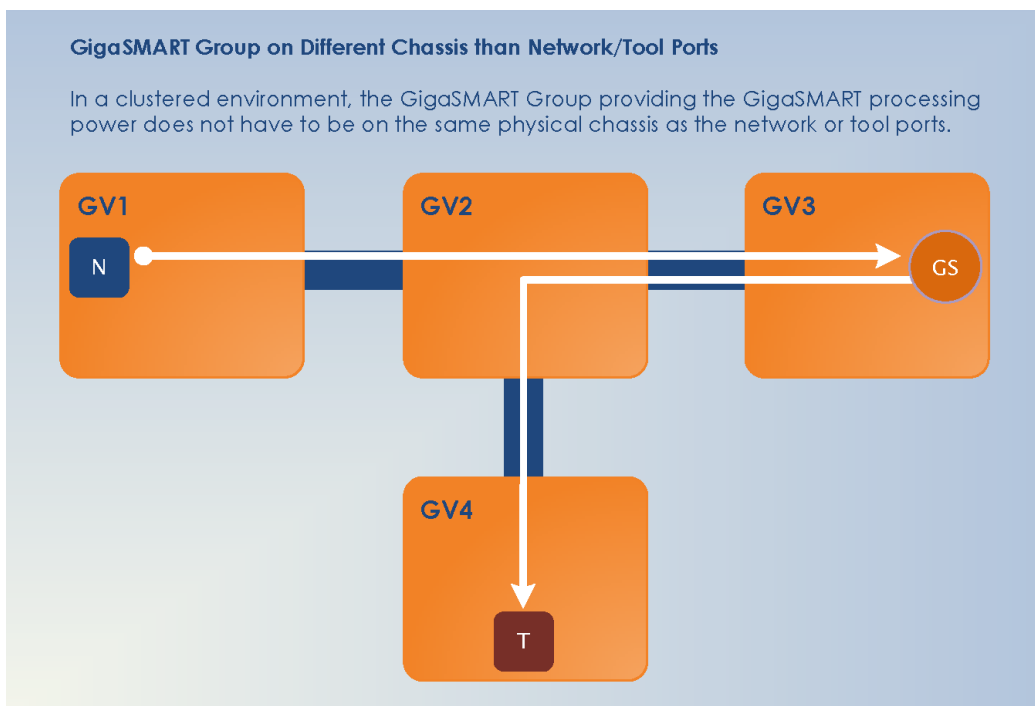


Figure 8 *GigaSMART Group on Different Chassis than Network/Tool Ports*

You could also have the GigaSMART group on the same chassis as either the network or tool ports for the map. An example of this is shown in Figure 9 [GigaSMART Operations in Clusters](#). The GigaSMART group on GV3 is on the same chassis as the egress port.

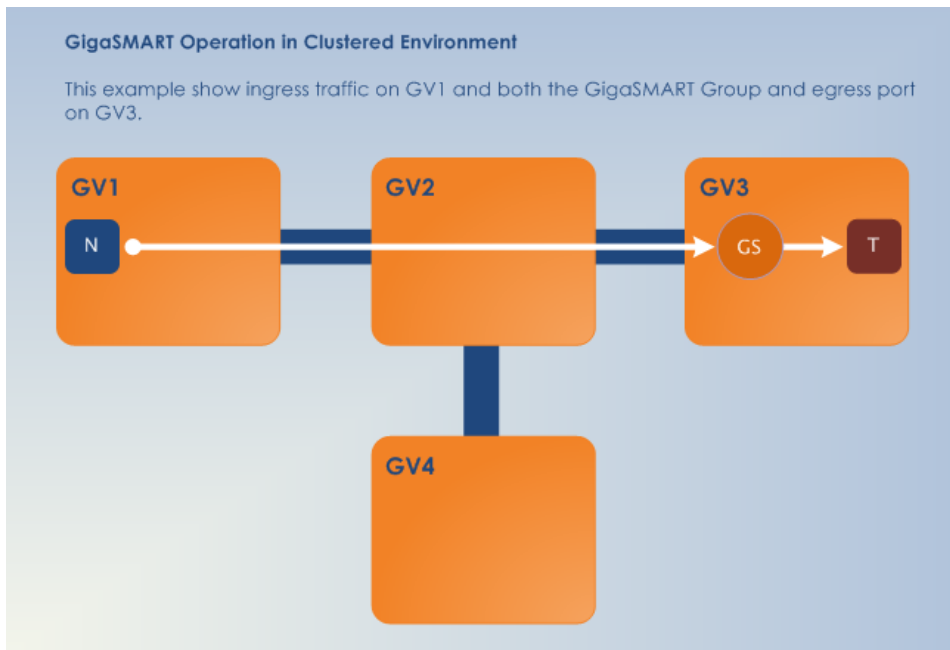


Figure 9 *GigaSMART Operations in Clusters*

How to Combine GigaSMART Operations

You can combine multiple GigaSMART components into a single operation. For example, you can set up a single GigaSMART operation that masks a packet, strips its VLAN header, and inserts a field in the GigaSMART Trailer.

The following table summarizes the valid combinations of GigaSMART operations.

Supported GSOP Combinations		Masking	Trailer Addition (Source Port Labeling)	Trailer Removal (Source Port Labeling)	De-Dup	Load Balance	App Filtering	App Intelligence		Flow-Ops				Headers			NetFlow		Slicing		SSL /TLS			Tunnels	
							APF	AFI (APF+ASF)	AMI	FlowVUE	GTP Flow Filter	GTP Whitelist	GTP Flow Sampling	Strip Headers	Add Headers	Remove HIT	NetFlow 1st level	NetFlow 2nd level	Slicing	Advanced Flow Slicing	SSL Decrypt	iSSL	ICAP	Tunnel Encap	Tunnel Decap
Masking			S	S	S	S	S	S	NS	S	NS	NS	NS	S	S	S	NS	NS	S	S	NS	NS	NS	S	S
Trailer Addition (Source Port Labeling)		S			S	S	S	NS	NS	S	NS	NS	NS	S	S	S	NS	NS	S	S	NS	NS	NS	S	S
Trailer Removal (Source Port Labeling)		S			S	S	S	NS	NS	S	NS	NS	NS	S	S	S	NS	NS	NS	NS	NS	NS	NS	S	S
De-Dup		S	S	S		S	S	S	S	S	NS	NS	NS	S	S	S	S	S	S	S	S	NS	NS	S	S
Load Balance		S	S	S	S		S	S	NS	S	S	S	S	S	S	S	NS	NS	S	S	NS	NS	NS	S	S
App Filtering	APF	S	S	S	S	S		NA	NS	S	NS	NS	NS	S	S	NS	NS	NS	S	S	NS	NS	NS	S	NS
App Intelligence	AFI (APF+ASF)	S	NS	NS	S	S	NA		S	NS	NS	NS	NS	NS	NS	NS	NS	S	S	S	NS	NS	NS	NS	NS
	AMI	NS	NS	NS	S	NS	NS	S		NS	NS	NS	NS	NS	NS	NS	NA	NA	NS	NS	NS	NS	NS	NS	NS
Flow- Ops	FlowVUE	S	S	S	S	S	S	NS	NS		NS	NS	NS	S	S	S	NS	NS	S	NS	NS	NS	NS	NS	NS
	GTP Flow Filter	NS	NS	NS	NS	S	NS	NS	NS	NS		S	NS	NS	NS	NS	NS	NS	S	NS	NS	NS	NS	NS	NS
	GTP Whitelist	NS	NS	NS	NS	S	NS	NS	NS	NS	S		NS	NS	NS	NS	NS	NS	S	NS	NS	NS	NS	NS	NS
	GTP Flow Sampling	NS	NS	NS	NS	S	NS	NS	NS	NS	NS	NS		NS	NS	NS	NS	NS	S	NS	NS	NS	NS	NS	NS
Headers	Strip Headers	S	S	S	S	S	S	NS	NS	S	NS	NS	NS		S	S	NS	NS	S	S	NS	NS	NS	S	S
	Add Headers	S	S	S	S	S	S	NS	NS	S	NS	NS	NS	S		S	NS	NS	S	S	NS	NS	NS	NS	S
	Remove HIT	S	S	S	S	S	NS	NS	NS	S	NS	NS	NS	S	S		NS	NS	NS	NS	NS	NS	NS	S	NS
NetFlow	NetFlow 1st level	NS	NS	NS	S	NS	NS	NS	NA	NS	NS	NS	NS	NS	NS	NS		NS	NS	NS	NS	NS	NS	NS	NS
	NetFlow 2nd level	NS	NS	NS	S	NS	NS	S	NA	NS	NS	NS	NS	NS	NS	NS	NS		NS	NS	NS	NS	NS	NS	NS
Slicing	Slicing	S	S	NS	S	S	S	S	S	S	S	S	S	S	S	S	NS	NS		S	NS	NS	NS	S	S
	Advanced Flow Slicing	S	S	NS	S	S	S	S	NS	S	S	S	S	S	S	S	NS	NS	S		NS	NS	NS	S	S
SSL/ TLS	SSL Decrypt	NS	NS	NS	S	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS		NS	NS	NS	NS
	iSSL	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS		NS	NS	NS
	ICAP	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS		NS	NS
Tunnels	Tunnel Encap	S	S	S	S	S	S	NS	NS	NS	NS	NS	NS	S	NS	S	NS	NS	S	S	NS	NS	NS		NS
	Tunnel Decap	S	S*	S	S	S	NS	NS	NS	NS	NS	NS	NS	S	S	NS	NS	NS	S	S	NS	NS	NS	NS	
								NS		=		Not Supported				NA		=		Not Applicable					
		S*				=		Supported for Gen 3 cards only																	

NOTE: Masking operations cannot be combined with slicing unless the offset of the slicing is after the offset of the masking.

How to Read GigaSMART Operations Table

The GigaSMART operations table is read both across and down. The following is an example of how to read the GigaSMART operations table:

1. Begin in the left-most column and select a GigaSMART operation, for example: Add Header.
2. Move to the right along the Add Header row. Add Header can be combined with Slicing or Masking, Source Id, Header/Trailer Remove, De-duplication, Tunnel decapsulation, and Strip Header. It cannot be combined with Tunnel Encap.

3. Move to the right another square to the gray square at end of the Add Header row. This is the Add Header column.
4. Move down the Add Header column, below the gray square at the end of the Add Header row. Add Header can be combined with Flow-Ops (FlowVUE), APF, ASF, and Load Balance. It cannot be combined with Flow-Ops (Flow-Filter GTP), Flow-Ops (GTP Whitelist), Flow-Ops (GTP Flow Sampling), NetFlow (1st Level Maps), NetFlow (2nd Level Maps), SSL Decryption (for Out-of-Band Tools), Inline-SSL (SSL Decryption for Inline Tools), Flow-Ops (SIP Flow Sampling), or Flow-Ops (SIP Flow Whitelist).

Work with GigaSMART Operation Combinations in GigaVUE-FM

When combining GigaSMART operations in GigaVUE-FM, the drop down option in the GSOP screen will gray out if a set of combinations is invalid.

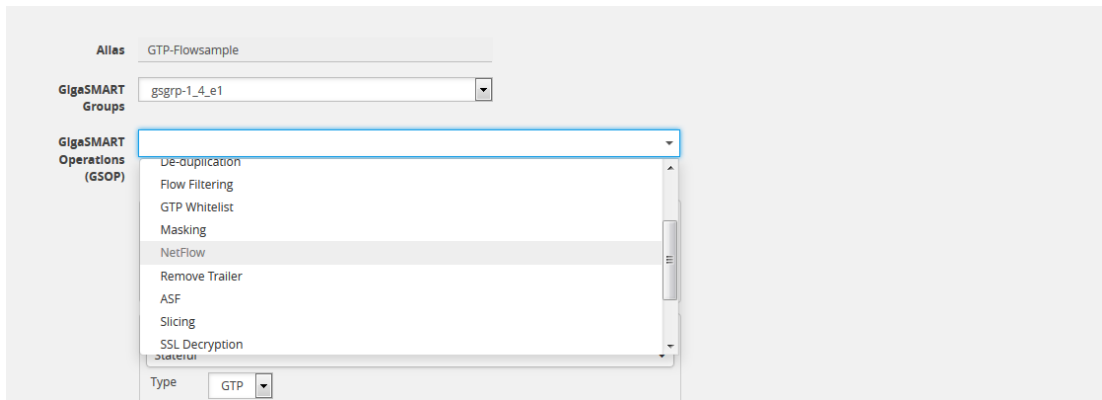


Figure 10 GigaSMART Operation Combinations Not Available

However, in certain cases you may not see the combinations grayed out but when trying to save the combination a pop-up is displayed stating that the combination is invalid.

To get the valid combinations, refer to the table at the beginning of this section that summarizes the combinations.

Supported GigaSMART Operations

The following topics lists the supported GigaSMART operations by GigaSMART physical and virtual nodes.

- Supported GigaSMART Operations on GigaVUE HC Series
- Supported GigaSMART Operations

Supported GigaSMART Operations on GigaVUE HC Series

NOTE: An initialization/deinitialization delay is encountered while configuring or removing configuration of a Passive SSL GSOP in new the Generation 3 GigaSMART card.

GigaSMART Operation	GigaVUE-HC1		GigaVUE-HC3		GigaVUE-HC1 Plus		GigaVUE-HCT
	Gen 2 On-board	Gen 3 SMT-HC1-S	Gen 2 (C05)	Gen 3 (C08)	Rear Gen3 SMT-HC1A-R	Front Gen 3 SMT-HC1-S	Gen 3 SMT-HC1-S
GigaSMART Masking	✓	✓	✓	✓	✓	✓	✓
GigaSMART Packet Slicing	✓	✓	✓	✓	✓	✓	✓
GigaSMART Advanced Flow Slicing	✓	✓	✓	✓	✓	✓	✓
Source ID (add Trailer)	✓	✓	✓	✓	✓	✓	✓
Header/Trailer Remove	✓	✓	✓	✓	✓	✓	✓
GigaSMART 5G CUPS	✗	✗	✓	✓	✗	✗	✗
De-Duplication	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Encapsulation	✓	✓	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE-HC1		GigaVUE-HC3		GigaVUE-HC1 Plus		GigaVUE-HCT
	Gen 2 On-board	Gen 3 SMT-HC1-S	Gen 2 (C05)	Gen 3 (C08)	Rear Gen3 SMT-HC1A-R	Front Gen 3 SMT-HC1-S	Gen 3 SMT-HC1-S
GigaSMART VxLAN Tunnel Encapsulation	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Decapsulation	✓	✓	✓	✓	✓	✓	✓
GigaSMART VXLAN Tunnel Decapsulation	✓	✓	✓	✓	✓	✓	✓
GigaSMART ERSPAN Tunnel Decapsulation	✓	✓	✓	✓	✓	✓	✓
GigaSMART IP Encapsulation	✓	✗	✓	✗	✗	✗	✗
GigaSMART IP Decapsulation	✓	✗	✓	✗	✗	✗	✗
Header Stripping	✓	✓	✓	✓	✓	✓	✓
Header Addition	✓	✓	✓	✓	✓	✓	✓
FlowVUE (IP-based)	✓	✓	✓	✓	✓	✓	✗
GTP Flow Filtering	✗	✗	✓	✗	✗	✗	✗
GigaSMART GTP Rotational Sampling	✗	✗	✓	✓	✓	✓	✗
GTP Whitelisting (GigaSMART GTP Rotational Sampling)	✗	✗	✓	✓ Non-CUPS GTP Correlation is supported. LTE CUPS is released as BETA* in 6.1.	✓	✓	✗
GTP Flow	✗	✗	✓	✓	✓	✓	✗

GigaSMART Operation	GigaVUE-HC1		GigaVUE-HC3		GigaVUE-HC1 Plus		GigaVUE-HCT
	Gen 2 On-board	Gen 3 SMT-HC1-S	Gen 2 (C05)	Gen 3 (C08)	Rear Gen3 SMT-HC1A-R	Front Gen 3 SMT-HC1-S	Gen 3 SMT-HC1-S
Sampling (GigaSMART GTP Rotational Sampling)				Non-CUPS GTP Correlation is supported. LTE CUPS is released as BETA* in 6.1.			
Adaptive Packet Filtering (APF) NOTE: Generation 3 nodes do not support RegEx masking.	✓	✓	✓	✓	✓	✓	✓
Application Session Filtering (ASF) and Buffer ASF	✓	✓	✓	✓	✓	✓	✓
Application Filtering Intelligence (AFI)	✓	✓	✓	✓	✓	✓	✓
Application Metadata Intelligence (AMI)	✓	✓	✓	✓	✓	✓	✓
GigaSMART NetFlow Generation (Application Intelligence)	✓	✓	✓	✓	✓	✓	✓
Application Visualization	✓	✓	✓	✓	✓	✓	✓
NetFlow (Traffic Intelligence)	✓	✗	✓	✗	✗	✗	✗
Load Balancing (Stateless)	✓	✓	✓	✓	✓	✓	✓
Load Balancing	✓	✓	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE-HC1		GigaVUE-HC3		GigaVUE-HC1 Plus		GigaVUE-HCT
	Gen 2 On-board	Gen 3 SMT-HC1-S	Gen 2 (C05)	Gen 3 (C08)	Rear Gen3 SMT-HC1A-R	Front Gen 3 SMT-HC1-S	Gen 3 SMT-HC1-S
(Stateful)							
SSL Decryption for Out-of-Band Tools (Passive SSL)	✓	✓	✓	✓	✓	✓	✓
SSL Decryption for Inline Tools	✓	✓	✓	✓	✓	✓	✗
SIP Flow Sampling	✗	✗	✓	✗	✓	✓	✗
SIP Flow Whitelist	✗	✗	✓	✗	✓	✓	✗
Stand-Alone User Processing Node Traffic Monitoring	✗	✗	✓	✓	✗	✗	✗
GigaSMART TCP tunnel Decapsulation	✓	✗	✓	✗	✗	✗	✗
Secure Tunnels Encapsulation	✗	✓	✗	✓	✓	✓	✓
Secure Tunnels Decapsulation	✗	✓	✗	✓	✓	✓	✓

*BETA features are available for functional Proof of Concepts only. Scalability and Performance limits will be available when the feature is released for formal deployments.

NOTE: The combination of Application Visualization, Application Filtering Intelligence (AFI), De-duplication, and Application Metadata Intelligence (AMI) is not supported for GigaVUE-HC1 Gen2 platform.

Order of GigaSMART Operations

When combining multiple GigaSMART components into a single operation, the components are applied in the following order:

1. [apf/asf/buffer asf] OR [flow-ops <flow-filtering>] or [flow-ops <gtp-whitelist>] or [flow-ops <gtp-flowsampling>] AND [lb] (Stateful load balancing with GTP or ASF)
2. [apf/asf/buffer asf (AFI)]
3. [tunnel-decap]
4. [dedup]
5. [ssl-decrypt]
6. [flow-ops <flow-sampling>]
7. [strip-header]
8. [slicing]
9. [enhanced slicing]
10. [masking]
11. [trailer]
12. [tunnel-encap]
13. [add-header]
14. [flow-ops <netflow>]
15. [lb] (Stateless load balancing)
16. metadata (AMI)

View GigaSMART Statistics

To view the GigaSMART statistics from the UI, select **GigaSMART Operations (GSOP) > Statistics**. The Statistics page displays as shown in [Figure 11GigaSMART Operations Statistics Page](#).

GSOP Alias	GS Group Alias	Map Alias	Rx Packets	Tx Packets	Rx Octets	Tx Octets	Packet Drops	Packet Drops No Init	Packets Terminated	Packets Parse Errors	GS Operations
GigavueVM_Tunnel	gsgrp-1_4_e1	OpenStack_vTraffic_toWireshark	3.23 M	60	814.48 M	7.26 K	3.23 M	0	0	0	Tunnel Decap
gtp_flow_sampling_elias_test	gsgrp-1_4_e1	GTP-Sampling-2	0	0	0	0	0	0	0	0	Flow Sampling

Figure 11 GigaSMART Operations Statistics Page

The Statistics page shows the aliases for GS Operation, GS Group, the alias of the map that is using GS Operation, and the GS Operations being used. In [Figure 11GigaSMART Operations Statistics Page](#), Flow Sampling and Load Balance operations are assigned to the alias GTP-Flowsample in the gsgrp-1_4_e1 GS Group. The GS operations is used by the map with the alias map-gtpFS. For a description of the other columns, refer to [GigaSMART Operations Statistics Definitions](#).

Other statistics available for viewing from the UI are the following:

- GigaSMART Groups Statistics (select **GigaSMART > Statistics**)

- NetFlow / IPF Generation Statistics for Exporters and Monitors (select **NetFlow / IPFIX > Exporter Statistics or NetFlow / IPFIX Generation > Monitor Statistics**)
- IP Interface Statistics (select **Ports > IP Interfaces > Statistics**)

NOTE: When tunnel load balancing is configured in Generation 3 GigaSMART card (SMT-HC1-S) with multiple maps using the same port-group, the GSOP statistics is the cumulative statistics of all the maps as the individual GSOP level statistics are not maintained in Generation 3 GigaSMART card (SMT-HC1-S).

Definitions of GigaSMART Statistics

The following sections provide definitions for the statistics displayed. Refer to the following:

- [NetFlow Monitor Statistics Definitions](#)
- [NetFlow Exporter Statistics Definitions](#)
- [IP Interfaces Statistics Definitions](#)
- [GigaSMART Group Statistics Definitions](#)
- [GigaSMART Group Flow Ops Report Statistics Definitions](#)
- [GigaSMART Operations Statistics Definitions](#)

NetFlow Monitor Statistics Definitions

To view NetFlow Monitor statistics, select **GigaSMART > NetFlow / IPFIX Generation > Monitor Statistics** to open the Monitor Statistics page.

The following table describes NetFlow Monitor statistics displayed on the Monitor Statistics page:

Statistic	Description
No Entries	The current number of flows in the monitor cache.
High Watermark	The maximum number of flows that have ever been in the monitor cache.
Flows Added	The sum of all flows added to the monitor cache.
Flows Aged	The sum of the flows that have aged due to the following: o Active Timeout—The configured active timeout for the

Statistic	Description
	monitor cache was exceeded. - o Inactive Timeout—The configured inactive timeout for the monitor cache was exceeded. - o Event Aged—The number of entries aged from the cache because a TCP FIN/RST flag was received. - o Watermark Aged—The number of entries aged from the cache because the CPU utilization of the cache exceeded 75%. - o Emergency Aged—The number of entries aged from the cache because a user requested a forced flush through the CLI.
No of Active Timeout	The number of times the configured active timeout for the monitor cache was exceeded.
No of Inactive Timeout	The number of times the configured inactive timeout for the monitor cache was exceeded.
No of Event Aged	The number of entries aged from the cache because a TCP FIN/RST flag was received.
No of Watermarked Aged	The number of entries aged from the cache because the CPU utilization of the cache exceeded 75%.
No of Emergency Aged	The number of entries aged from the cache because a user requested a forced flush through the CLI.

NetFlow Exporter Statistics Definitions

To view NetFlow Exporter statistics, select **GigaSMART > NetFlow / IPFIX Generation > Monitor Statistics** to open the Exporter Statistics page.

The following table describes NetFlow Exporter statistics:

Statistic	Description
Templates Added	The number of data templates added to the exporter.
Records Added	The number of data records added to the exporter.
Filtered Records Removed	The number of records filtered by exporter filters
Empty Records Not Added	The number of records not added to NetFlow because they were empty or blank.

Statistic	Description
	In the NetFlow record, if all the collect fields contain only enterprise extensions such as URL, HTTP, or DNS, and if during run-time, the records are blank or empty, they will be counted as Empty Records Not Added.
Packets Sent	The number of packets sent from the exporter to the collector.
Packet Dropped	The number of packets dropped, which could be due to the inability to send packets, such as there is no network connection or the port is down.
Packet Transmit Errors	The number of packets dropped, which could be due to the inability to send packets, such as there is no network connection or the port is down.

IP Interfaces Statistics Definitions

To view IP Interfaces statistics, select **Ports > IP Interfaces > Statistics** to open the IP Interfaces Statistics page. The statistics of the control traffic such as ARP, ICMP, and ICMPv6 for the physical node will be displayed. Use the **Clear** button to remove the selected IP interface statistics. Use the **Clear All** button to remove all the IP interface statistics. [Figure 12 IP Interfaces Statistics](#) shows an example.

IP Interface	Bytes Rx	Bytes Tx	Packets Rx	Packets Tx	Multicast Packets Rx	Discards Rx	Discards Tx	Errors Rx	Errors Tx	Overruns Rx	Overruns Tx	Frame Rx	Carrier Tx	Collisions Tx
ip1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ip2	0	148544	0	2321	0	0	0	0	0	0	0	0	0	0

Figure 12 IP Interfaces Statistics

The following table describes IP interfaces statistics:

Statistic	Description
IP Interface	The IP interface for which the statistics is displayed.
Bytes Rx	The number of bytes received into the IP interface.
Bytes Tx	The number of bytes transmitted out of the IP interface.
Packets Rx	The number of packets received into the IP interface.
Packets Tx	The number of packets transmitted out of the IP interface.
Multicast Packets Rx	The number of multicast packets received into the IP interface.
Discards Rx	The number of packets that were received and discarded by the IP interface.
Discards Tx	The number of packets that were transmitted out of the IP interface and were discarded.
Errors Rx	The number of packets with errors that were received into the IP interface.
Errors Tx	The number of packets with errors that were transmitted out of the IP interface.
Overruns Rx	The number of first-in-first-out (FIFO) buffer errors that were received into the IP interface.
Overruns Tx	The number of first-in-first-out (FIFO) buffer errors that were transmitted out of the IP interface.
Frame Rx	The number of frames received into the IP interface.
Carrier Tx	The number of packets in which carrier losses were detected when transmitted out of the IP interface.
Collisions Tx	The number of packets that were colliding when transmitted out of the IP interface.

TLS/SSL Application Statistics Definitions

The following table describes TLS/SSL application statistics:

Statistic	Description
active_sessions	The number of current active sessions.

Statistic	Description
num_session_ids_cached	The number of current session IDs that have been cached.
num_tls_tickets_cached	The number of current TLS tickets that have been cached.
total_sessions	The cumulative total number of sessions.
handshaked_sessions	The number of sessions that passed TLS/SSL handshake between a client and server to establish a session.
failed_sessions	The cumulative total number of failed sessions.
num_session_resumed_session_id	The total number of resumed sessions with a session ID.
num_session_resumed_ticket	The total number of resumed sessions with TLS tickets.
num_session_timedout	The number of TLS/SSL sessions that have timed out.
avg_in_pkts_per_session	The average number of input packets per session.
avg_out_pkts_per_session	The average number of output packets per session.

ASF Statistics Definitions

The following table describes ASF statistics:

Statistic	Description
Packet In	The number of packets received by the ASF application.
Session Created	The number of sessions created.
Session Freed	The number of sessions deleted.
Session Timeout	The number of sessions that were deleted due to inactivity (expiry of the session timer).
Packet Match Session	The number of incoming packets matching ASF sessions. This count does not include the packets that triggered the creation of the session.
Packets Buffered	The number of packets stored by buffer ASF prior to the APF match.
APF Match Pass	The number of packets matching a pass GigaSMART rule.

Statistic	Description
APF Match Drop	The number of packets matching a drop GigaSMART rule.
Packet Pass	The number of packets sent to tool ports due to a pass GigaSMART rule. (This includes packets belonging to pass sessions for ASF.)
Packet Drop	The number of packets dropped due to a drop GigaSMART rule. (This includes packets belonging to drop sessions for ASF.)
Packet No Match	The number of packets that did not match any GigaSMART rule. (This includes packets belonging to non-pass/drop sessions for ASF.)
Packets masking failures in this Map	Increases when a packet matches a regex rule with masking enabled, but the configured masking range (start/end offsets or length) does not result in a valid area to overwrite. The counter is updated at most once per packet, even if multiple regex gsrules in the same map match that packet.
Buffered Packet Pass	The number of buffered packets whose sessions matched a pass GigaSMART rule.
Buffered Packet Drop	The number of buffered packets whose sessions matched a drop GigaSMART rule.
Buffered Packet No Match	The number of buffered packets whose sessions did not match any GigaSMART rule.
Session Exceed Buffer Count	The number of sessions without an APF match after buffering that exceeded the configured buffer count.
Packet Exceed Buffer Count	The number of packets belonging to sessions that exceeded the configured buffer count.
Out of Buffer	The number of times GigaSMART ran out of packet buffer when trying to store a packet in a session.
Out of Session	The number of times GigaSMART ran out of session entries when trying to create a session.

GigaSMART Group Statistics Definitions

To view GigaSMART Group statistics, select **GigaSMART > GigaSMART Groups > Statistics** to open the Statistics page. [Figure 13GigaSMART Group Statistics](#) shows an example.

GS GROUP ALIAS	RX PACKETS	TX PACKETS	RX OCTETS	TX OCTETS	PACKET DROPS	RESOURCE OVERLO...	PACKETS RECEIVED ...	HEARTBEAT STATUS	HEARTBEAT RX PAC...	HEARTBEAT TX PAC...	TOTAL PORTS
dssl_gsgroup	140969438	50753016	32827384183	6328155248	70826411	No	0				1

Figure 13 GigaSMART Group Statistics

The following table describes GigaSMART group statistics:

Statistic	Description
Rx Packets	The cumulative number of packets coming into a GigaSMART group.
Tx Packets	The cumulative number of packets going out of a GigaSMART group.
Rx Octets	The cumulative number of bytes coming into a GigaSMART group.
Tx Octets	The cumulative number of bytes going out of a GigaSMART group.
Packet Drops	The cumulative number of packets dropped at a GigaSMART group.
Packet Received Errors	The cumulative number of received packets with errors at a GigaSMART group.
Heartbeat Status of eport	The status of heartbeat. The valid values are up, down, or NA. This heartbeat status is for a GigaSMART engine port on a GigaSMART group for inline TLS/SSL decryption On a supported platform, such as GigaVUE-HC3, the status will be either up or down, followed by number of packets sent and received. On an unsupported platform, the status will be NA and the number of packets will not be displayed. The heartbeat status for the GigaSMART cards is fully operational only when it is configured with the inline TLS/SSL application. In all other cases, the default value of the heartbeat status is Up and the status is generally ignored.
Heartbeat Rx Packets	The heartbeat receive packet count.
Heartbeat Tx Packets	The heartbeat transmit packet count.

NOTE: The K, M, G and T in the statistics page denote KiloBytes, MegaBytes, GigaBytes and TeraBytes, respectively. You can click on the GSOP alias to view the detailed statistics.

GigaSMART Group Flow Ops Report Statistics Definitions

The following sections provide definitions for the statistics that are reported for the GigaSMART group. Refer to the following:

- [Flow Ops Report Statistics Definitions for FlowVUE](#)
- [Flow Ops Report Statistics Definitions for GTP](#)
- [Flow Ops Report Statistics Definitions for GTP Overlap](#)
- [Flow Ops Report Definitions for SIP/RTP Correlation](#)
- [Flow Ops Report Statistics for Passive TLS/SSL Decryption](#)

Flow Ops Report Statistics Definitions for FlowVUE

The following table describes Flow Ops report statistics for FlowVUE:

Statistic	Description
From GigaVUE-OS-CLI	
Device IP	The IP address of the flow.
In Sample	The sample selected for pass (1) or drop (0).
Num Packets	The number of packets seen for the flow.
Num Octets	The sum of the packet lengths of all packets seen for the flow.
From GigaVUE-FM	
num_devices	The number of devices.
num_devices_in_sample	The number of devices in the sample.

Flow Ops Report Statistics Definitions for GTP

The following table describes Flow Ops report statistics for GTP, including GTP flow filtering, GTP whitelisting, and GTP flow sampling:

Statistic	Description
Tunnel[Ver]	The tunnel type (CTRL for control plane, USER for user data)

Statistic	Description
	plane) and version (1 or 2).
Interface EBI:LBID[QCI]	The interface and Evolved Packet System (EPS) Bearer Identifier (EBI), Linked Bearer Identity (LBI), and QoS Class Identifier.
IP:Tunnel-ID ==> IP:Tunnel-ID	The IP addresses and tunnel identifiers of both sides of the tunnel. Note: For LTE nodes only, the IP addresses can be both IPv4 and IPv6.
IMSI	The International Mobile Subscriber Identity (IMSI) value.
APN	The Access Point Name (APN) value.
WL	The IMSI had a match in the forward list (WL) or did not. The values are N for no and Y for yes.
FS	The IMSI was flow sampled or not. The values are A for accepted, R for rejected, and N for no match.
ID	The rule ID of the flow sample rule.
LB port	The load balancing port number.
Pkts	The number of packets.
Timestamp	The internal clock time of when the session was created.
GTP Resource Summary	
Num Sessions In Use	The number of correlated session in use.
Num Tunnels In Use	The number of used tunnels in the tunnel resource pool.
Tunnels Available	The number of available tunnels in the tunnel resource pool.
UPN CTunnels Available	The number of available tunnels in the UPN C tunnels resource pool.
Tunnels Pending Free	The number of tunnels marked free, ready to be returned to the tunnel resource pool.
Tunnels Marked Free	The number of times used tunnels are marked free.
Tunnels Returned	The number of times used tunnels are returned to the tunnel resource pool.
Current Time	The current time (in CPU cycles). Used for debugging.
Flow Filtering Report Summary	
Control Tunnels	The total number control tunnels.

Statistic	Description
Control & User Tunnels	The total number of control and user tunnels.
GTP Session Stats	The interface type: Gn/Gp, S1U/S11, S5/S8, S3/S4, or Other.
Sessions	The number of sessions by interface. Note the following: - The counter for S3/S4 will always be 0 (not supported). - The S10 interface is counted under Other.
Tunnels	The number of tunnels by interface.
Pending Session	The number of sessions waiting for control message response.
Control Only Session	The number of sessions without user bearers.
Flow Sampling Report Summary	
Total Devices	The total number devices in the flow sample
Number of Device in Sample	The number of devices used in each sample session
Flow SIP Report Summary	
SIP Sessions	This graph displays the total sessions, total sessions in use and the number of parse errors.
RTP Sessions	This graph displays the total number of sessions and the total data pool in use.
GTP Interface Stats	
For overlap maps, refer to the notes below the table for Flow Ops Report Statistics Definitions for GTP Overlap	
Rx Pkts	The received (Rx) packets for GTP correlation statistics for GTP traffic by interface type: S11, S1u, S5S8 (control and user), Gn (control and user), total (control and user), collector (control and user). Note: If traffic does not match any map rules, it will be sent to the collector.
Rx Bytes	The received (Rx) bytes for GTP correlation statistics for GTP traffic by interface type.
Sample/WL/Filter (Tx) Pkts	The transmitted (Tx) packets sampled in for flow sampling, forward listing, and flow filtering by interface type. For example, if sampling is 60%, then 60% is sampled in.
Sample/WL/Filter (Tx)	The transmitted (Tx) bytes sampled in for flow sampling,

Statistic	Description
Bytes	forward listing, and flow filtering by interface type.
Sample Out (Dropped) Pkts	The packets sampled out (dropped) by interface type. For example, if sampling is 60%, then 40% is sampled out.
Sample Out (Dropped) Bytes	The bytes sampled out (dropped) by interface type.
Xaui Drop	The total traffic (Rx bytes and packets) dropped due to oversubscription on the interface into the GigaSMART.

Statistics for Control Message (GTP-c)

GTPV1	The GTPv1 (version 1) message type.
Cre PDP Req	Create Packet Data Protocol (PDP) context request.
Cre PDP Rsp	Create PDP context response.
Upd PDP Req	Update PDP context request.
Upd PDP Rsp	Update PDP context response.
Del PDP Req	Delete PDP context request.
Del PDP Rsp	Delete PDP context response.
GTPV2	The GTPv2 (version 2) message type.
Cre Ssn Req	Create session request.
Cre Ssn Rsp	Create session response.
Mod Bea Req	Modify bearer request.
Mod Bea Rsp	Modify bearer response.
Del Ssn Req	Delete session request.
Del Ssn Rsp	Delete session response.
Cre Bea Req	Create bearer request.
Cre Bea Rsp	Create bearer response.
Upd Bea Req	Update bearer request.
Upd Bea Rsp	Update bearer response.
Del Bea Req	Delete bearer request.
Del Bea Rsp	Delete bearer response.
Mod Bea Cmd	Modify bearer command.

Statistic	Description
Mod Bea Fai	Modify bearer failure indication.
Bea Rsr Cmd	Bearer resource command.
Bea Rsr Fai	Bearer resource failure indication.
Message Counters	
Tool Pass	The number of control messages passed to the tools.
Col NoSess	The number of control messages sent to the collector without matching sessions.
Col NoTnlx	The number of “out of tunnels” requests sent to the collector for the control message.
Col ParseEr	The number of control messages sent to the collector with unsupported options.
Col NoRule	The number of control messages sent to the collector without matching rules.
Col Other	The number of control messages sent to the collector with other conditions, for example, the message matched a drop rule.
Statistics for User Data Message (GTP-u)	
Tool Pass	The number of user data messages passed to the tools.
Collector	The number of user data messages sent to the collector without matching sessions.
Drop	The number of user data messages dropped.

Flow Ops Report Statistics Definitions for GTP Overlap

The following table describes Flow Ops report statistics for GTP overlap flow sampling. Since most fields are the same as [Flow Ops Report Statistics Definitions for GTP on page 719](#), they are not repeated. Refer to the note below the table for GTP Interface Stats for overlap maps.

Statistic	Description
Tunnel[Ver]	The tunnel type (CTRL for control plane, USER for user data plane) and version (1 or 2).

Statistic	Description
Interface EBI:LBI[QCI]	The interface and Evolved Packet System (EPS) Bearer Identifier (EBI), Linked Bearer Identity (LBI), and QoS Class Identifier.
IP:Tunnel-ID ==> IP:Tunnel-ID	The IP addresses and tunnel identifiers of both sides of the tunnel.
IMSI	The International Mobile Subscriber Identity (IMSI) value.
APN	The Access Point Name (APN) value.
Overlap Result	The overlap result. A map group for GTP overlap flow sampling maps contains six maps. Each character in the result represents one of the maps. The result is in alphabetical order for each map within the map group. (There is no map priority.) Refer to the following legend: ▪ A—Flow Sample Accept ▪ R—Flow Sample Reject ▪ W—Whitelist Accept ▪ N—No Match
Pkts	The number of packets.
Timestamp	The internal clock time of when the session was created.

The following notes are for the combination of overlap and non-overlap maps:

- If at least one flow sample map accepts the packets among all the pairs of overlap maps, the Sample (Tx) counters in the GTP Interface Stats will be incremented. If more than one pair of maps accepts the packets the Sample (Tx) counters in the GTP Interface Stats will still be incremented only once.
- If at least one forward list map matches the packets among all the pairs of overlap maps, the Sample (Tx) counters in the GTP Interface Stats will be incremented. If more than one pair of maps matches the packets the Sample (Tx) counters in the GTP Interface Stats will still be incremented only once.
- If there are no forward list maps and all flow sample maps are no-rule-match, the Sample (Tx) and Sample Out counters in the GTP Interface Stats will not be incremented.

Flow Ops Report Definitions for SIP/RTP Correlation

The following table describes Flow Ops report statistics for SIP/RTP correlation.

Statistic	Description
PROTO	The protocol, such as SIP, RTP, or RTCP. Note: The RTCP port number is assumed to be the corresponding RTP port number plus 1. This results in even numbered RTP ports and odd numbered RTCP ports.
TRANSPORT	The transport layer, such as UDP or TCP.
METHOD	The SIP method (or SIP message).
CALLER: IP	The corresponding IP address of the caller.
CALLEE: IP	The corresponding IP address of the callee.
PDU	The number of packets seen for this session.
CALL-ID	The call identifier.
WL	The caller/callee ID had a match in the whitelist (WL) or did not. The values are N for no and Y for yes.
FS	The caller ID was flow sampled or not. The values are A for accepted, R for rejected, and N for no match.
ID	The rule ID
LB port	The load balancing port number, which is the port over which the session has been load balanced. All SIP and corresponding RTP packets will be sent to this port.
Timestamp	The internal clock time of when the session was created.
Message counters	
SIP messages	All the SIP messages that have been correlated, such as, ACK, BYE 200, CANCEL, INFO, and so on. These counters are cumulative
Tool Pass	The number of SIP messages passed to the tools
NoSess	The number of SIP messages sent to the collector without matching sessions
NoRule	The number of SIP messages sent to the collector without matching rules.
NoMatch	Reserved
Other	The number of SIP messages sent to the collector with other conditions.

Statistic	Description
SIP Resource Summary	
Num Sessions In Use	The number of SIP sessions.
Sessions Available	The number of remaining SIP sessions available. (This varies by GigaSMART node.)
RTP Resource Summary	
Num Data Pools In Use	The number of RTP sessions.
Data Pools Available	The number of remaining RTP sessions available. (This varies by GigaSMART node.)

Flow Ops Report Statistics for Passive TLS/SSL Decryption

The following table describes Flow Ops report statistics for Passive SSL decryption:

Statistic	Description
Session Summary	
GsGroup	The GigaSMART group associated with the passive TLS/SSL decryption.
Total Sessions	The total number of passive TLS/SSL decryption sessions.
SSLv3 Sessions	The cumulative total number of SSL 3.0 sessions.
TLS1.0 Sessions	The cumulative total number of TLS 1.0 sessions.
TLS 1.1 Sessions	The cumulative total number of TLS 1.1 sessions.
TLS 1.2 Sessions	The cumulative total number of TLS 1.2 sessions.
Session IDs	The number of current session IDs.
Tickets	The number of current TLS tickets.
Report Summary	The link to the Report Summary page that displays the graphical representation of the passive TLS/SSL decryption session summary.
Session Details	
Server IP	The IP address of the server.

Statistic	Description
Server Port	The port number of the server.
Client IP	The IP address of the client.
Client Port	The port number of the client.
Version	The version of the SSL/TLS protocol.
First Error	The first error encountered on a session. After the first error, subsequent packets are dropped. If a session encounters errors, the packets for that session are ignored. The session will be cleared after the session times out.
First Error Reason	The reason for the first error encountered on a session.
In Packets	The number of packets going into the session.
Out Packets	The number of packets transmitted out of the session.
SNI	The TLS server name indication (SNI).
Decryption Status	The passive TLS/SSL decryption status.
Start Time	The session start time.
Duration	The duration of the session.
Finger Print	The finger print is applicable only for certificate-based TLS/SSL decryption session.
Cipher Suite	The cipher suite details used to decrypt the session.

GigaSMART Operations Statistics Definitions

To view GigaSMART Operations statistics, select **GigaSMART > GigaSMART Operations (GSOP) > Statistics** to open the Statistics page.

The following table describes the statistics that are common to all GigaSMART operations:

Statistic	Description
Pkts Drop	The cumulative number of packets dropped at a GigaSMART operation for a map.
Pkts Rx	The cumulative number of packets coming into a GigaSMART operation for a map.

Statistic	Description
Octets Rx	The cumulative number of bytes coming into a GigaSMART operation for a map.
Pkts Term	The cumulative number of packets of a terminated session of a GigaSMART operation for a map.
Octets Tx	The cumulative number of bytes going out of a GigaSMART operation for a map.
Pkts Tx	The cumulative number of packets going out of a GigaSMART operation for a map.
Pkts Drop No Init	For internal debugging.
Pkts Parse Err	The cumulative number of packets with invalid or unsupported header types of a GigaSMART operation for a map.

The following sections provide definitions for the statistics that are specific to a particular GigaSMART operation. Refer to the following:

- [Passive TLS/SSL Decryption Statistics Definitions](#)
- [Inline TLS/SSL Decryption Statistics Definitions](#)
- [De-duplication Statistics Definitions](#)
- [ERSPAN Statistics Definitions](#)
- [Tunnel Decapsulation Statistics Definitions](#)
- [Tunnel Encapsulation Statistics Definitions](#)
- [APF Statistics Definitions](#)
- [ASF Statistics Definitions](#)
- [Masking Statistics Definitions](#)
- [Slicing Statistics Definitions](#)
- [Header Stripping Statistics Definitions](#)
- [Generic Header Stripping Statistics Definitions](#)
- [Trailer Statistics Definitions](#)
- [FlowVUE Statistics Definitions](#)
- [NetFlow Statistics Definitions](#)

Passive TLS/SSL Decryption Statistics Definitions

The following table describes GigaSMART operations statistics for Passive TLS/SSL decryption:

Statistic	Description
Sessions Total	The cumulative total number of sessions.
Sessions Active	The number of currently active sessions.

Inline TLS/SSL Decryption Statistics Definitions

The statistics for inline TLS/SSL decryption are described in [Work With Inline TLS/SSL Decryption](#).

De-duplication Statistics Definitions

The following table describes GigaSMART operations statistics for de-duplication (including the statistics that are displayed in a cluster environment):

Statistic	Description
Ip 6 Missed Op Busy	For IPv6 packets, the number of non-duplicate packets passed through without storing because the GigaSMART engine was too busy processing other packets. Note: Applies only to non-duplicate packets.
Non Ip Dupl	The number of non-IPv4 and non-IPv6 duplicate packets detected.
Non Ip	The number of non-IPv4 and non-IPv6 packets received for de-duplication.
Ip 6 Missed Op Space	For IPv6 packets, the number of non-duplicate packets passed through without storing because the GigaSMART engine did not have enough storage space. Note: Applies only to non-duplicate packets.
Non Ip Missed Op Busy	For non-IPv4 and non-IPv6 packets, the number of non-duplicate packets passed through without storing because the GigaSMART engine was too busy processing other packets. Note: Applies only to non-duplicate packets.
Non Ip Missed Op Space	For non-IPv4 and non-IPv6 packets, the number of non-duplicate packets passed through without storing because the GigaSMART engine did not have enough storage space. Note: Applies only to non-duplicate packets.

Statistic	Description
Ip 4 Missed Op Busy	For IPv4 packets, the number of non-duplicate packets passed through without storing because the GigaSMART engine was too busy processing other packets. Note: Applies only to non-duplicate packets.
Ip 4 Missed Op Space	For IPv4 packets, the number of non-duplicate packets passed through without storing because the GigaSMART engine did not have enough storage space. Note: Applies only to non-duplicate packets.
Ip 4 Ipid Tcp Rst	The number of TCP RESETs for IPv4 plus TCP packets. (IPv4 plus TCP RESET packets are not de-duplicated.)
Ip 6 Dupl	The number of IPv6 duplicate packets detected.
Ip 4 Dupl	The number of IPv4 duplicate packets detected.

ERSPAN Statistics Definitions

The following table describes GigaSMART operations statistics for ERSPAN tunnel:

Statistic	Description
Drop Type 3 Marker Bad Sig	The number of ERSPAN Type III packets that have a bad marker packet signature. The expected marker packet signature is 0xa5a5a5a5.
Pkts Too Big	The number of ERSPAN packets that are larger than 9600 bytes after the timestamp trailer is added. These packets will be dropped.
Pkts Rx Type 3	The total number of ERSPAN Type III packets received.
Pkts Tx Type 3 Marker	The total number of ERSPAN Type III marker packets received. (These packets are not forwarded.)
Pkts Rx Type 2	The total number of ERSPAN Type II packets received.
Type 3 Marker Overdue	The number of ERSPAN Type III marker packets that are overdue. Based on granularity, if a marker packet does not arrive by the time specified, it is considered overdue. Refer to ERSPAN Granularity .
pkts Rx	The total number of ERSPAN packets received into the IP interface.
Drop Unknown Proto	The number of packets dropped because they were not

Statistic	Description
	recognized as ERSPAN packets or ERSPAN marker packets.
Drop Id No Hit	The number of ERSPAN packets with a wrong flow ID/ERSPAN ID.

Tunnel Decapsulation Statistics Definitions

The following table describes GigaSMART operations statistics for tunnel decapsulation:

Statistic	Description
GMIP Tunnel	
Drop Wrong Addr	The number of GMIP tunneled packets dropped whose destination UDP port does not match the configured value.
Drop Other	The number of GMIP tunneled packets dropped because of fragmented packets.
Pkts Rx	The number of packets received into the IP interface.
Reassemble Rx Success	The number of incoming packets successfully reassembled.
Drop Unknown Proto	The number of packets through the network IP interface dropped if they are neither IPv4 or UDP packets.
Reassemble Rx	The number of incoming packets to be reassembled.
Drop Reassemble Mem Full	The number of packets not successfully reassembled and dropped due to lack of memory for reassembly.
Sliced Mtu	Not valid for tunnel decapsulation.
Drop Reassemble Max Hold	The number of packets not successfully reassembled and dropped due to the arrival of too many fragments not yet reassembled. The maximum fragment sessions are already held for reassembly.
Drop No Arp	The number of packets dropped because ARP was not resolved on the IP interface (in particular, on a tool IP interface).
Drop Reassemble Overlap Frag	The number of packets not successfully reassembled and dropped due to overlapping reassembly fragments.

Statistic	Description
L2GRE Decap Tunnel	
Drop Key Mismatch	The number of packets dropped due to key mismatch.
Pkts Rx	The number of packets received into the IP interface.
Reassemble Rx Success	The number of incoming packets successfully reassembled.
Drop Unknown Proto	The number of packets dropped due to an unknown protocol.
Reassemble Rx	The number of incoming packets to be reassembled.
Drop Reassemble Mem Full	The number of packets not successfully reassembled and dropped due to lack of memory for reassembly.
Drop Reassemble Max Hold	The number of packets not successfully reassembled and dropped due to the arrival of too many fragments not yet reassembled. The maximum fragment sessions are already held for reassembly.
Drop Other	The number of packets dropped due to other reasons.
Drop Reassemble Overlap Frag	The number of packets not successfully reassembled and dropped due to overlapping reassembly fragments.
Pkts Too Big	The number of packets that are larger than 9000 bytes after the timestamp trailer is added. These packets will be dropped.

Tunnel Encapsulation Statistics Definitions

The following table describes GigaSMART operations statistics for tunnel encapsulation:

Statistic	Description
GMIP Encap Tunnel	
Fragment Rx	The number of incoming packets to be fragmented.
Drop Other	Not valid for tunnel encapsulation.
Pkts Rx	The number of packets received into the IP interface.
Fragment Tx	The number of outgoing packets sent to the tunnel after

Statistic	Description
	fragmentation.
Sliced Mtu	The number of packets that are sliced to the MTU size of the tool IP interface.
Drop No Arp	The number of packets dropped because ARP was not resolved on the IP interface (in particular, on a tool IP interface).
L2GRE Encap Tunnel	
Fragment Rx	The number of incoming packets to be fragmented.
Pkts Rx	The number of packets received into the IP interface.
Fragment Tx	The number of outgoing packets sent to the tunnel after fragmentation.
Session Current Total	The number of currently active sessions.
Session Alloc Fail	The number of session allocations that failed.
Session Lookup	The number of lookups in a session.
Session Lookup Success	The number of lookups in a session that were a success.
Session Alloc	The number of sessions allocated.
Session Timedout	The number of sessions that timed out after a configured timer value.
Sliced Mtu	The number of packets that are sliced to the MTU size of the tool IP interface.
Drop No Arp	The number of packets dropped because ARP was not resolved on the IP interface (in particular, on a tool IP interface).
CUSTOM Decap Tunnel	
rx_packets	The number of packets received into the IP interface.
pkts_drop_unknown_protocol	The number of packets dropped due to an unknown protocol.
pkts_drop_portsrc_mismatch	The number of packets dropped due to source port mismatch.
pkts_drop_portdst_mismatch	The number of packets dropped due to destination port mismatch.
pkts_in_reassemble	The number of incoming packets to be reassembled.
pkts_in_reassemble_success	The number of incoming packets successfully reassembled. For example, if four (4) packets are reassembled into one (1), 4 is displayed in this field.
pkts_out_reassembled	The actual number of packets sent out the tool port. For example, if four (4) packets are reassembled into one (1), 1 is displayed in this

Statistic	Description
	field.
pkts_drop_reassemble_overlap_frag	The number of packets not successfully reassembled and dropped due to overlapping reassembly fragments.
pkts_drop_reassemble_max_hold	The number of packets not successfully reassembled and dropped due to the arrival of too many fragments not yet reassembled. The maximum fragment sessions are already held for reassembly.
pkts_drop_reassemble_mem_full	The number of packets not successfully reassembled and dropped due to lack of memory for reassembly.
pkts_drop_reassemble_timed_out	The number of packets dropped due to timeout in the reassembly queue.
VXLAN Decap Tunnel	
rx_packets	The number of packets received into the IP interface.
pkts_drop_unknown_protocol	The number of packets dropped due to an unknown protocol.
pkts_drop_portsrc_mismatch	The number of packets dropped due to source port mismatch.
pkts_drop_portdst_mismatch	The number of packets dropped due to destination port mismatch.
pkts_in_reassemble	The number of incoming packets to be reassembled.
pkts_in_reassemble_success	The number of incoming packets successfully reassembled. For example, if four (4) packets are reassembled into one (1), 4 is displayed in this field.
pkts_out_reassembled	The actual number of packets sent out the tool port. For example, if four (4) packets are reassembled into one (1), 1 is displayed in this field.
pkts_drop_reassemble_overlap_frag	The number of packets not successfully reassembled and dropped due to overlapping reassembly fragments.
pkts_drop_reassemble_max_hold	The number of packets not successfully reassembled and dropped due to the arrival of too many fragments not yet reassembled. The maximum fragment sessions are already held for reassembly.
pkts_drop_reassemble_mem_full	The number of packets not successfully reassembled and dropped due to lack of memory for reassembly.
pkts_drop_reassemble_timed_out	The number of packets dropped due to timeout in the reassembly queue.
pkts_too_big	The number of packets that are larger than 9000 bytes after the timestamp trailer is added. These packets will be dropped.

APF Statistics Definitions

The following table describes GigaSMART operations statistics for APF:

Statistic	Description
Apf Drop	The number of packets matching the GigaSMART drop rules.
Apf Pass	The number of packets matching the GigaSMART pass rules.
Rule Not Match	The number of packets not matching any GigaSMART rules in the map.
Masking Err	The number of masking errors in the map. This number is usually zero (0), which indicates no issues with the masking operation. If the number is non-zero, it indicates there is some issue with the masking operation.

ASF Statistics Definitions

The following table describes GigaSMART operations statistics for ASF:

Statistic	Description
Session Created	The number of sessions created.
Session Deleted	The number of sessions deleted.
Session Timeout	The number of sessions that were deleted due to inactivity (expiry of the session timer).
Session Matched (pkt)	The number of incoming packets matching ASF sessions. This count does not include the packets that triggered the creation of the session.
Exceed Count Drop	The number of packets dropped, even if they matched a flow session, because a packet-count was configured and exceeded.

Masking Statistics Definitions

The following table describes GigaSMART operations statistics for masking:

Statistic	Description
No Header	The number of packets with no configured masking protocol.
Too Short	The number of packets with a length less than the masking offset.

Slicing Statistics Definitions

The following table describes GigaSMART operations statistics for slicing:

Statistic	Description
No Header	The number of packets with no configured header for slicing.
Too Short	The number of packets with a length less than the slicing length.
Min Len	The number of packets that are sliced to less than 64 bytes.

Header Stripping Statistics Definitions

The following table describes GigaSMART operations statistics for Header Stripping:

Statistic	Description
Id No Hit	The number of packets that do not match the configured VXLAN ID to be stripped.
Fm 6000 Pkts Ts	The number of packets received with the FM6000 timestamp.
Unknown Next	The number of packets not stripped of their configured header type as the packets will have an unknown header after the header is stripped.
No Header	The number of packets with no configured header type to be stripped.
Fm 6000 Data Pkt Too Big	The number of FM6000 packets that are larger than 9600 bytes after the timestamp trailer is added. These packets will be dropped.

Statistic	Description
Fm 6000 Keyframe Overdue	The number of FM6000 key frames that are overdue. By default, the key frame rate is 1 packet per second. If a key frame is not received in 1 second, this statistic is incremented.
Fm 6000 Keyframe	The number of key frames received from the FM6000 device. Key frames are marker packets that carry information to convert the FM6000 timestamp to UTC time.

Generic Header Stripping Statistics Definitions

The following table describes GigaSMART operations statistics for generic Header Stripping:

Statistic	Description
first_anchor_header_not_present	The number of packets with no configured first anchor header.
offset_beyond_anchor_header_size	The number of packets that are not stripped as the configured offset size exceeds the size of the first anchor header.
second_anchor_header_not_present	The number of packets with no configured second anchor header.
strip_length_beyond_pkt_len	The number of packets that are not stripped as the configured strip length exceeds the packet length.
strip_success	The number of packets that are successfully stripped.
incompatible_anchor_headers	The number of packets that are dropped as the first anchor header is incompatible with the second anchor header after the stripping operation is complete.

Trailer Statistics Definitions

The following table describes GigaSMART operations statistics for trailers:

Statistic	Description
pkts_too_big	The number of packets for which the size of the packet has

Statistic	Description
	become greater than the maximum supported size (9600) when adding the trailer. This count is incremented with one trailer added to the packet.

FlowVUE Statistics Definitions

The following table describes GigaSMART operations statistics for FlowVUE:

Statistic	Description
Dev Ip Src Match	The number of packets with a source IP matching the range defined in the GigaSMART parameters (gsparams).
Exceed License Warn	The number flows that exceed the installed license.
Exceed License Err	The number of flows that exceed the installed license error limit. (The limit is the number of sessions in the license plus 5%.)
Dev Ip No Match	The number of packets with a source and destination IP that does not match any of the ranges defined in the GigaSMART parameters (gsparams).
Dev Ip Non Ip	The number of packets with no IP headers (and hence, not sampled).
Dev Ip Dst Match	The number of packets with a destination IP matching the range defined in the GigaSMART parameters (gsparams).
Out of Resource	The number of times there was a failure to allocate resources for recording a new flow. Note: The maximum supported flows for each engineport is 2 million.
Dev Ip Drop Not In Sample	The number of packets dropped by the sampling application, not because of errors, but because the flow was sampled to be dropped.

NetFlow Statistics Definitions

The following table describes GigaSMART operations statistics for NetFlow:

Statistic	Description
Out of Resource	The number of times there was a failure to allocate resources for recording a new flow. Note: The maximum supported flows for each engine port is 2 million.
Non Ip	The number of packets received that are not IPv4 or IPv6.
Non Configured	Packets received when NetFlow is not enabled in the GigaSMART group.
TLS/SSL Active Sessions	The number of currently active TLS/SSL sessions monitored by NetFlow.
Total TLS/SSL Sessions	The cumulative total number of TLS/SSL sessions monitored by NetFlow.

Display GigaSMART Application Resource Usage

GigaSMART applications, such as De-duplication and inline and Passive SSL decryption, use memory resources on the GigaSMART line card or module. As new GigaSMART applications are configured, the total resources on the GigaSMART line card or module can become fully used.

Starting in software version 4.4, you can display the GigaSMART application resource usage, which provides information about the applications that use resources. With this information, you can choose to free up resources on one application to use them on another.

Table 1: GigaSMART Application Resource Information

Name	Format
GSgroup	The alias of the GigaSMART group associated with the GigaSMART application.
Application	The list of licensed GigaSMART applications that use resources, including Adaptive Packet Filtering (APF), de-duplication, GPRS Tunneling Protocol (GTP), NetFlow Generation, Passive SSL decryption, Adaptive Session Filtering (ASF) with buffering, and inline SSL decryption. Other GigaSMART applications (such as flow sampling, header addition, Header Stripping, ERSPAN tunnel decapsulation, slicing, masking, and others) do not have databases that store data, therefore they do not use resources and are not displayed with the show gsgroup gsapp-resource command.

Name	Format
% of Total	The percentage of the total amount of memory used by each GigaSMART application.
Configured Resource	The amount of resources configured for each GigaSMART application. The valid values are as follows: ▪ app-max—Indicates the maximum amount of memory configured for the application. It is a pre-allocated amount. ▪ integer, such as 2—Indicates the number of sessions configured, in the units specified. M indicates millions.
Installed Resource	The amount of resources installed for each GigaSMART application.
Licensed Quantity	The amount of resources licensed for each GigaSMART application.
Units	The units, such as sessions, or millions (M) of sessions.

Overview of GigaSMART Application Resources

GigaSMART application resources are managed per GigaSMART group (gsgroup). A gsgroup can be configured with one or more GigaSMART engine ports on one or more GigaSMART line cards or modules.

For most GigaSMART applications, resources are allocated automatically, based on configuration. For some GigaSMART applications, resources are allocated when they are configured in the gsgroup. For other applications, resources are allocated when a GigaSMART operation (gsop) using the application is created. For buffer ASF however, you can explicitly configure resources, in millions of sessions.

The allocation of resources for a new application will be successful if the application is licensed and if there is sufficient space for the new application.

If there is insufficient space, then the resources need to be managed to free up memory for the new application. Managing resources includes deleting applications that are no longer used.

However, deleting a GigaSMART application does not result in the immediate deletion of application resources. Once a resource has been allocated, it remains allocated. To delete resources for APF, out-of-band or inline SSL decryption, de-duplication, and GTP, remove the configuration related to the application, then reload the GigaSMART line card or module.

To remove the configuration related to an application, delete the gsop first, then delete the gsgroup. If the gsop or gsgroup is bound to a map, you will also have to delete the map.

Resources for Buffer ASF

The resources for buffer ASF depend on the number of sessions and the type of node. For example, GigaVUE-HC3, 5 million sessions uses 26%.

For GigaVUE-HC3, the resources for buffer ASF for the number of sessions is as follows:

- 2 million—11% of total resources
- 3 million—16% of total resources
- 4 million—21% of total resources
- 5 million—26% of total resources

Reload GigaSMART Line Card or Module

Occasionally, the GigaSMART line card or module will need to be reloaded for changes to take effect and to allocate resources accordingly. Reloading also provides applications with contiguous memory.

The following message displays at the bottom of the output of the **show gsgroup gsapp-resource** command when the GigaSMART line card or module needs to be reloaded:

```
*Resource allocation changes have been made that require GigaSMART card 2/1/1 to be reloaded in order for them to take effect.
```

When this message is displayed, you cannot change the configuration relating to that application until after the reload. For example, you cannot use the gsop, associated with the gsgroup, in a map.

Use the following command to reload a GigaSMART line card or module:

(config) # card slot <slot ID> down

Use the following command to bring the GigaSMART line card or module back up:

(config) # no card slot <slot ID> down

GigaSMART CPU Utilization Statistics

You can display CPU utilization statistics for GigaSMART. The statistics indicate the performance of GigaSMART, improve visibility, and help identify high load conditions.

Show commands display instantaneous CPU utilization as well as historical, providing trends for CPU utilization.

You can also configure a rising threshold, as a percentage, to indicate when high CPU utilization occurs. When the aggregate CPU utilization percentage exceeds the rising threshold, an SNMP notification can be triggered.

This feature is supported on all products that support GigaSMART: GigaVUE-HC1 and GigaVUE-HC3.

The GigaSMART engine port (**e** port) numbers are e1 on nodes with one GigaSMART engine and e1 and e2 on nodes with two GigaSMART engines, for example: 10/1/e1 or 8/1/e1 and 8/1/e2.

Refer to the following sections for viewing statistics, configuring the threshold, and configuring a notification that can be sent when the threshold is exceeded:

- [Display GigaSMART CPU Utilization](#)
- [Configure Threshold](#)
- [Configure Threshold Crossing Notification](#)

Display GigaSMART CPU Utilization

Use the **show gsgroup stats all** command to display the statistics on all GigaSMART groups on the node.

The statistics are displayed for 1 second, 1 minute, 5 minute, 10 minute, and 15 minute intervals. The 1 second interval displays the statistics for the previous second. The 1 minute, 5 minute, 10 minute, and 15 minute intervals display statistics containing history.

Statistics are displayed in an aggregate form. For example, if there are two GigaSMART **e** ports: e1 and e2, there will be two aggregates. One aggregate will be for e1, the other will be for e2. The term aggregate refers to aggregation across all packet processing cores (up to 31) in the CPU. It does not refer to an aggregate across CPUs.

The statistics are as follows:

- Useful Time—Amount of time during which the CPU is processing packets, in milliseconds (ms) or seconds (s).
- Idle Time—Amount of time during which the CPU is not processing packets, for example, when it is busy looping, in milliseconds (ms) or seconds (s).
- In Packets (pkts/s)—Number of packets per second coming into the CPU. For the 1 second interval, In Packets is the actual number of incoming packets for that second. For the 1 minute, 5 minute, 10 minute, and 15 minute intervals, In Packets is an average number of incoming packets per second.
- Packets Drop (pkts/s)—Number of packets per second dropped by the CPU. For the 1 second interval, Packets Drop is the actual number of dropped packets for that second. For the 1 minute, 5 minute, 10 minute, and 15 minute intervals, Packets Drop is an average number of dropped packets per second.
- Packets Recv Error—Number of received packets per second with errors. For the 1 second interval, Packets Recv Error is the actual number of errored packets for that second. For the 1 minute, 5 minute, 10 minute, and 15 minute intervals, Packets Recv Error is an average number of errored packets per second.
- CPU Usage %—Percentage of time during which the CPU is processing packets. CPU Usage % plus CPU Idle % equals 100.
- CPU Idle %—Percentage of time during which the CPU is not processing packets. CPU Idle % plus CPU Usage % equals 100.

NOTE: When the node is restarted, the 1 minute, 5 minute, 10 minute, and 15 minute statistics will not be exactly for 1 minute, 5 minute, 10 minute, and 15 minute intervals, until the full interval has elapsed and the history is available.

Configure Threshold

An upper threshold (rising) can be configured. When the aggregate value of the CPU utilization on the GigaSMART engine exceeds the threshold, an SNMP notification can be triggered. Refer to [Configure Threshold Crossing Notification](#).

Configure Threshold Crossing Notification

When the aggregate value of the CPU utilization exceeds the upper (rising) threshold, a message is logged, and optionally, an SNMP notification is sent to all configured destinations.

When enabled, the SNMP notification is sent when the rising threshold is exceeded in any 5-second interval over which the CPU utilization is averaged.

NOTE: Once the rising threshold is exceeded for 5 seconds, the SNMP notification is generated. However, if the CPU utilization falls below the upper threshold but does not remain below that threshold continuously for 5 seconds, a new notification is not generated when the upper threshold is exceeded again. A new notification is generated only when the CPU utilization falls below the threshold, stays below the threshold continuously for 5 seconds, exceeds the threshold again, and stays above it for 5 seconds.

How to Use GigaSMART Trailers

Required License: Base

Supported Devices : GigaVUE-HC1 Gen 2, GigaVUE-HC1 Gen 3, GigaVUE-HC3 Gen 2, GigaVUE-HC3 Gen 3, GigaVUE-HC1-Plus, and GigaVUE-HCT

GigaSMART operations can add the GigaSMART Trailer to packets, providing metadata on where the packet was processed.

GigaSMART Trailers can be combined with other GigaSMART operations. Refer to [How to Combine GigaSMART Operations](#) for the valid combinations.

If a trailer is included, it can optionally include the original packet's CRC as one field and a Source ID (Source port label) as another. The Source ID indicates where the packet entered the GigaSMART H Series node and how it was processed. The modified packet's actual CRC is always recalculated to reflect its new length. Refer to the [Source ID Field](#) for information.

Trailer operations can be assigned to GigaSMART groups consisting of multiple engine ports. Refer to [Groups of GigaSMART Engine Ports](#) for details.

Refer to [Supported GigaSMART Operations](#) for more details on the devices that support GigaSMART operations.

Source ID Field

When you enable the **Source ID** field for the GigaSMART Trailer, the trailer includes an additional field that identifies the platform type, box ID, slot number, and port number of the network port where the packet entered the GigaSMART H Series node. Refer to [Format of the GIGAMON_SRCID TLV](#) for the exact details.

Keep in mind the following when configuring GigaSMART operations with a **Source ID** argument:

Feature	Description
Source ID Field in GigaSMART Trailer	The Source ID field in the Gigamon Trailer includes the following values: - o Platform Type – The type of GigaSMART node where the packet was first seen. - o Group ID – The cluster ID/group ID configured for the node on which the packet was received. The GigaSMART H Series uses cluster IDs. - o Box ID – The box ID is configured for the GigaSMART node on which the packet was received. Box IDs are used for the unique identification of nodes in a cluster. NOTE: The box ID field in the Gigamon Trailer supports box ID values from 1-63, inclusive. - o Slot ID – The slot ID for the port on which the packet was received. - o Port ID – The physical port number on which the packet was received.

Example – GigaSMART Source Port Labeling with a GigaSMART Trailer

This example creates a GigaSMART operation named **src_headermask** with **Masking** and **Trailer** components. This operation will mask packets using a static masking offset of 148 bytes that continues for the next 81 bytes, writing over the existing data with an FF pattern. Then it attaches a GigaSMART Trailer indicating the original size of the packet before masking, the original packet's CRC, and the box ID, slot ID, and port ID of the physical input port on the GigaSMART H Series node. [Figure 14GigaSMART Operation with Masking and Trailer Components](#) shows the GigaSMART operation with masking and trailer components.

The screenshot displays the GigaSMART configuration interface. At the top, the 'Alias' field is set to 'src_headermask'. Below it, the 'GS Groups' dropdown menu is set to 'gsgrp1'. The 'GS Operations' field is empty. Two expandable sections are visible: 'Add Trailer' and 'Masking'. The 'Add Trailer' section is expanded, showing 'CRC' and 'Source ID' both checked. The 'Masking' section is also expanded, showing a dropdown set to 'None', 'Offset' set to 148, 'Pattern' set to 'FF', and 'Length' set to 81.

Figure 14 *GigaSMART Operation with Masking and Trailer Components*

Remove GigaSMART Trailers

You can also construct GigaSMART operations that remove the GigaSMART Trailer from packets. These operations are useful in cases where you have cascade connections – a tool port receiving packets with a GigaSMART trailer is physically cabled to a GigaSMART H Series network port, sending the packets received on the tool port back into a GigaSMART H Series node. You may want to remove the GigaSMART trailer before the packets are forwarded to other tools – that is when the special **Remove Trailer** argument comes in handy. [Figure 15 Remove Trailer Enabled](#) shows Remove Trailer enabled for a GigaSMART operation.

The screenshot displays the GigaSMART configuration interface, similar to Figure 14. The 'Alias' field is 'src_headermask' and 'GS Groups' is 'gsgrp1'. The 'GS Operations' field is empty. The 'Remove Trailer' section is expanded, showing the 'Enabled' checkbox checked.

Figure 15 *Remove Trailer Enabled*

Example: Removing GigaSMART Trailers in a Cascade

Figure 16 Cascade Physically Cabled from Tool to Network Port and Figure 17 Removing the GigaSMART Trailer from a Cascade Connection illustrate a situation where a GigaSMART operation that removes the GigaSMART trailer would be useful. Consider the physical deployment shown in Figure 16 Cascade Physically Cabled from Tool to Network Port:

- The **green** illustrates a one-way cascade between a tool (output) port (port 1/1/x12) and a network (input) port (port 1/1/x9).
- If traffic arriving on port 1/1/x12 includes a GigaSMART Trailer, you may want to use a **Trailer Remove** GigaSMART operation to remove it before logically forwarding traffic from port 1/1/x9 to another port on the GigaSMART.

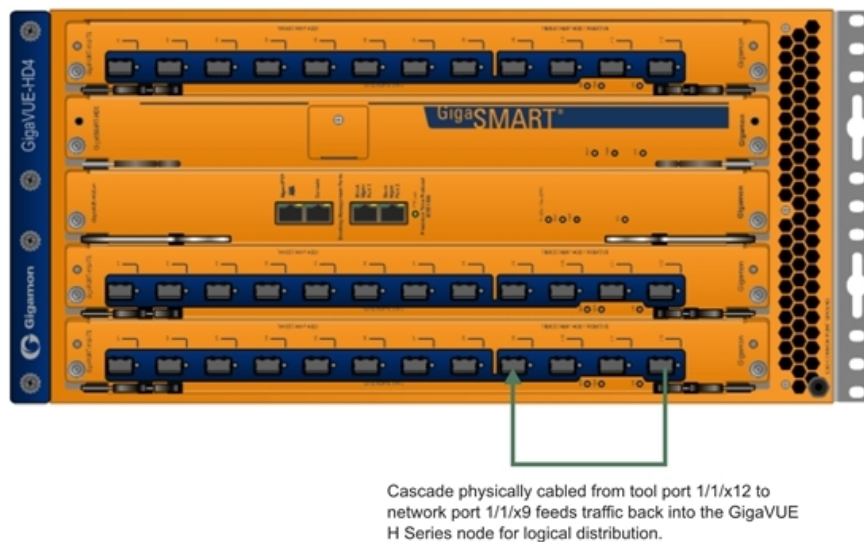


Figure 16 Cascade Physically Cabled from Tool to Network Port

For example, consider the packet distribution shown in Figure 17 Removing the GigaSMART Trailer from a Cascade Connection:

- The map named **add_trailer** is bound to network port 1/1/x1..x2. It adds the GigaSMART trailer and sends it to tool ports 1/1/x5..x8.
- Tool ports 1/1/x5..x7 are all connected to tools that expect the extra data in the GigaSMART Trailer.
- Tool port 1/1/x8 is physically cabled to network port 1/1/x4 in a cascade. To remove the GigaSMART Trailer from packets arriving on this port before they are forwarded to tool port 1/1/x9, we have bound a map named **no_trailer** to network port 1/1/x4 that is configured to remove the GigaSMART Trailers from all arriving packets.
- Tool port 1/1/x9 receives packets without the GigaSMART Trailer attached.

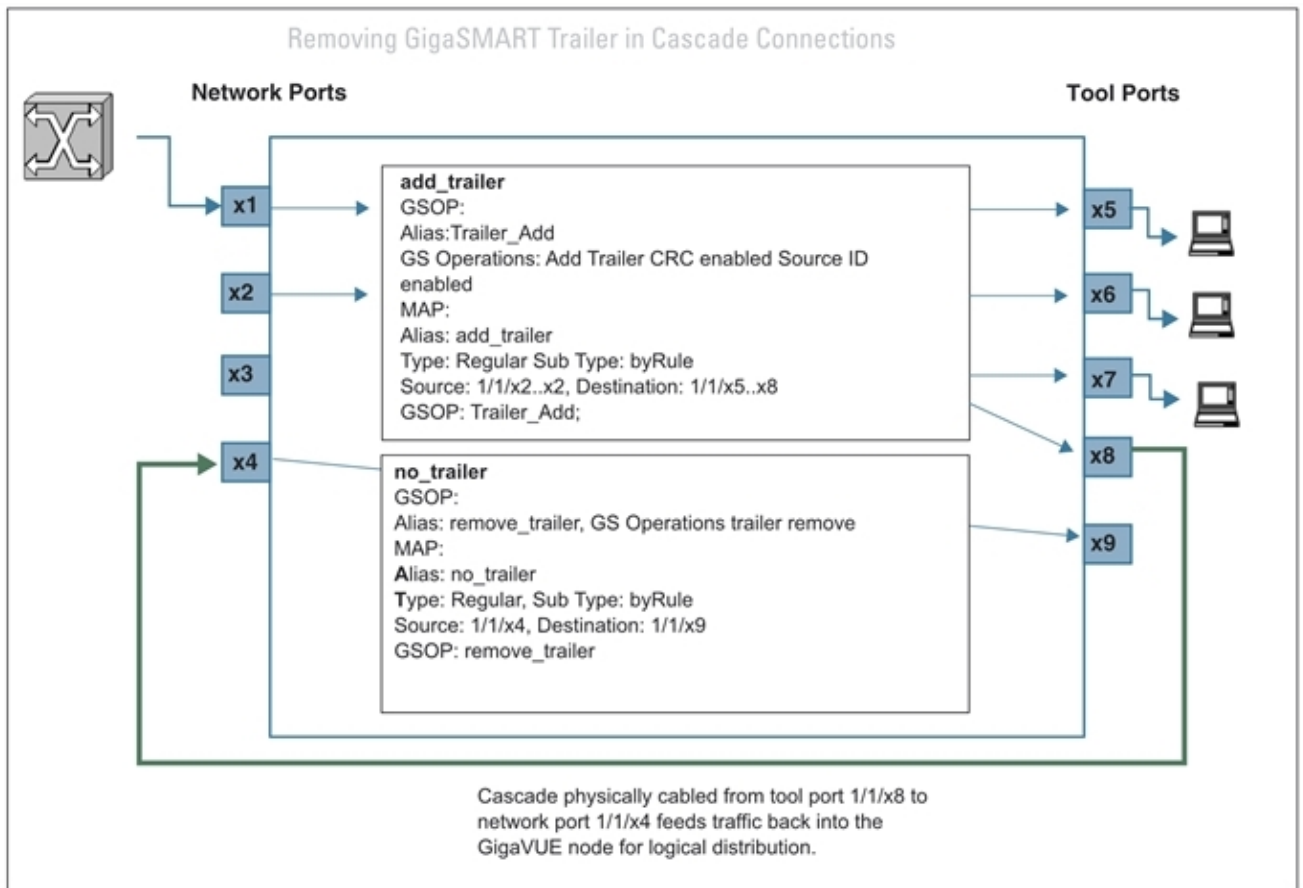


Figure 17 Removing the GigaSMART Trailer from a Cascade Connection

Multiple GigaSMART Trailers and Cascade Connections

Cascade connections also make it possible for multiple GigaSMART trailers to be attached to the same packet. For example, consider the cascade shown in [Figure 17 Removing the GigaSMART Trailer from a Cascade Connection](#) and suppose that instead of the **no_trailer** map removing the GigaSMART Trailer on packets arriving over the cascade physically cabled from tool port 1/1/x8, there is a second GigaSMART operation adding another trailer. In cases like this, the GigaSMART adds the most recent trailer at the end of the packet.

The same principle works for the **Remove Trailer** operations:

- The most recent trailer is removed from the end of the packet. Any other trailers are left intact by a single Remove operation.

Interpret GigaSMART Trailer

The trailer inserted by the GigaSMART line card can be interpreted using a recent version of the Wireshark[®] Protocol Analyzer. Refer to the [GigaSMART Trailer Reference](#) for details on the GigaSMART Trailer and its TLVs.

GigaSMART Trailer Reference

This section provides reference information on the format, position, and contents of the Gigamon Ethertype and GigaSMART Trailer fields in a packet processed by the GigaSMART-HD0 line card.

Refer to [How to Use GigaSMART Trailers](#) for details on how the GigaSMART Trailer is used in packets.

GigaSMART Trailer Format

This section describes the format of the GigaSMART Trailer. [Figure 18GigaSMART Trailer Format](#) summarizes the position and contents of the GigaSMART Trailer and the Gigamon Ethertype field (0x22E5).

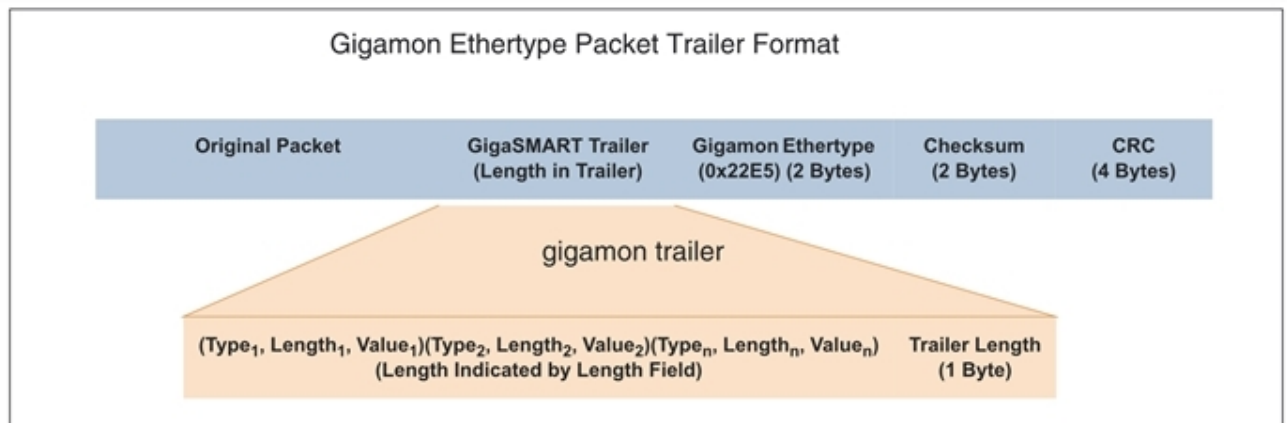


Figure 18 *GigaSMART Trailer Format*

GigaSMART Trailer Format

GigaSMART operations can insert metadata as a trailer at the end of the packet. As shown in the following figure, the GigaSMART Trailer consists of one or more TLVs, followed by the Trailer Length Field. The GigaSMART Trailer is followed by the Gigamon

Ethertype, a Checksum, and a recalculated CRC for the packet.

(Type1, Length1, Value1) (Type2, Length2, Value2) (Type(n), Length(n), Value(n)) (Length Indicated by Length Field)	Trailer Length(1 Byte)	Gigamon Ethertype (0x22E5) (2 Bytes)	Checksum(2 Bytes)
---	------------------------	--------------------------------------	-------------------

[Table 2: Gigamon Trailer Format](#) lists and describes each of the fields in the GigaSMART Trailer:

Table 2: Gigamon Trailer Format

Field	Description
TLVs	TLVs are used to carry the metadata inserted by GigaSMART operations. Within a TLV, the Type and Length fields are each one byte long. The length field indicates the size of the Value field. Refer to GigaSMART Trailer TLVs for a summary of the available TLVs and their formats.
Length	Specifies the size of the GigaSMART trailer. The Trailer Length does not include the length bytes
Gigamon Ethertype	Two-byte field identifying packet modified by GigaSMART line card. Value is 0x22E5. Protocol analysis equipment can use the Gigamon Ethertype in the trailer to find the start of the trailer: • Move one byte to the left to find the Trailer Length Field. • Read the number of bytes for the Trailer Length and move the number of bytes specified to the left to find the start of the Trailer.
Checksum	Two-byte field used to validate that the extra data is, in fact, a trailer and not random data with the Gigamon Ethertype.

GigaSMART Trailer TLVs

This section lists and describes the format of the Gigamon TLVs used in this release. TLVs are used to carry the metadata inserted by GigaSMART operations. Within a TLV, the Type and Length fields are each one byte long. The size of the Value field is indicated by the Length field.

Table 3: Gigamon TLVs

Tag Type	TLV ID	Value Field Length (Bytes)	Description
GIGAMON_PKT_LEN	1	2	Original Packet Length This TLV is included in any packet with a GigaSMART Trailer – adding the Trailer changes the original packet length.
GIGAMON_SRCID_G	2	3	Original Packet Source Identifier This TLV is included in any packet processed by a GigaSMART operation configured to include the Source ID (Source port label) field as part of its trailer. Refer to Format of the GIGAMON_SRCID TLV for a description of how the physical input source is encoded.
GIGAMON_CRC	7	4	Original Packet CRC This TLV is included in any packet processed by a GSOP configured to include the original packet's CRC as part of its trailer (If the CRC option is selected in the Trailer Add argument).
GIGAMON_SRCID	8	4	Original Packet Source Identifier (GigaSMART H Series) This TLV is included in any packet processed by a GigaSMART line card on a GigaSMART H Series node configured to include the Source ID (Source port label) field as part of its trailer (If the SRCID option is selected in the Trailer Add argument). Refer to Format of the GIGAMON_SRCID TLV for a description of how the physical input source is encoded.

Format of the GIGAMON_SRCID TLV

The GIGAMON_SRCID TLV is included in any packet processed by a **Source ID**(Source port label) GigaSMART operation. The GIGAMON_SRCID TLV consists of 3 bytes indicating the platform type, group ID, box ID, and port ID for the physical port where the packet entered the GigaSMART H Series node:

GIGAMON_SRCID TLV (32 Bits/4 Bytes)				
Platform(6 Bits)	Group ID (4 Bits)	Box ID(6 Bits)	Slot ID(6 Bits)	Port ID(10 Bits)

Name	Description	Bits
Platform	The type of GigaSMART node where the packet was first	6

Name	Description	Bits
	seen. Can be one of the following: - o Unknown - o GigaVUE-HCT - o GigaVUE-HC1 - o GigaVUE-HC1-Plus - o GigaVUE-HC3 - o GigaVUE-TA25 - o GigaVUE-TA25E - o GigaVUE-TA100 - o GigaSMART-TA200 - o GigaVUE-TA200E - o GigaVUE-TA400 - o GigaVUE-TA400E For bitmapping details, refer to the Platform Mapping	
Group ID	The “Group Id” ranges between 0 and 15. For standalone devices, it is set to 0 and for the devices in a cluster, it reports the corresponding cluster ID.	4
Box ID	Box IDs are used to uniquely identify nodes in a cluster. Standalone systems typically have a default box ID of 1 here. NOTE: The box ID field in the Gigamon Trailer supports box ID values from 0-63, inclusive. Box IDs within the range 1 to 63 will be displayed in the SRC TLV. For any other value, the Box ID will be shown as zero.	6
Slot ID	The number of the slot including the physical port for the packet.	6
Port ID	The physical input port number for the packet. Refer to Port ID Values by Line Card Type for a summary of the values used by GigaSMART H Series line card.	10

Platform Mapping

The following table summarizes the bitmapping details for the platforms:

Platform	Ports SCRID Value for Platform Type
GMON_GS_CHASSIS_TYPE_HCT	26

Platform	Ports SCRID Value for Platform Type
GMON_GS_CHASSIS_TYPE_HC1	15
GMON_GS_CHASSIS_TYPE_HC1P	16
GMON_GS_CHASSIS_TYPE_HC3	17
GMON_GS_CHASSIS_TYPE_TA25	21
GMON_GS_CHASSIS_TYPE_TA25E	25
GMON_GS_CHASSIS_TYPE_TA100	13
GMON_GS_CHASSIS_TYPE_TA200	19
GMON_GS_CHASSIS_TYPE_TA200E	24
GMON_GS_CHASSIS_TYPE_TA400	23

Port ID Values by Line Card Type

The following table summarizes the values inserted in the GIGAMON_SRCID TLV for the port ID by GigaSMART device and the line card type:

GigaSMART Device / Line Card	Ports	Port IDs Inserted in Gigamon Trailer
GigaVUE-HC1 Gen 2		
HC1-X12G4	x1..x12	5..16
	g1..g4	1..4
BPS-HC1-D25A24	x1..x4	53..56
	x5..x8	49..52
PRT-HC1-X12	x1..x12	49..60
GigaVUE-HC3 Gen 2		
PRT-HC3-X24	x1..x24	1..24
PRT-HC3-C08Q16	c1..c8	1, 5, 9, 13, 17, 21, 25, 29
PRT-HC3-C08Q16-4x10Gb	c1x1-x4.. c8x1-x4	1..32

GigaSMART Device / Line Card	Ports	Port IDs Inserted in Gigamon Trailer
Mode		
PRT-HC3-C08Q16-4x25Gb Mode on Control Card Version 2	c1x1-x4.. c8x1-x4	1..32
SMT-HC3-C05	c1..c5	1, 5, 9, 13, 17
SMT-HC3-C05-4x10Gb Mode	c1x1-x4.. c5x1-x4	1..20
SMT-HC3-C05-4x25Gb Mode on Control Card Version 2	c1x1-x4.. c5x1-x4	1..20
BPS-HC3-C25F2G	x1..x16	1..16
	c1..c4	17, 21, 25, 29
BPS-HC3-C35F2G	x1..x16	1..16
	c1..c4	17, 21, 25, 29
BPS-HC3-Q35F2G	x1..x16	1..16
	q1..q4	17, 21, 25, 29
PRT-HC3-C16	c1..c16	1, 5, 6, 10, 11, 15, 16, 20, 21, 25, 26, 30, 31, 35, 36, 40
PRT-HC3-C16-4x10Gb Mode	c1x1..x4	1..4
	c3x1..x4	6..9
	c5x1..x4	11..14
	c7x1..x4	16..19
	c9x1..x4	21..24
	c11x1..x4	26..29
	c13x1..x4	31..34
	c15x1..x4	36..39

GigaSMART Device / Line Card	Ports	Port IDs Inserted in Gigamon Trailer
PRT-HC3-C16-4x25Gb Mode	c1x1..x4	1..4
	c3x1..x4	6..9
	c5x1..x4	11..14
	c7x1..x4	16..19
	c9x1..x4	21..24
	c11x1..x4	26..29
	c13x1..x4	31..34
	c15x1..x4	36..39

GigaVUE-HC1 Gen 3

HC1-X12G4	g1..g4	1..4
	x1..x12	5..16
PRT-HC1-X12	x1..x12	1..12
PRT-HC1-Q04X08	c1..c4	25, 29, 37, 33
	x1..x8	41..48

GigaVUE-HC3 Gen 3

PRT-HC3-X24	x1..x24	1..24
PRT-HC3-C08Q08	c1..c8	1, 5, 9, 13, 17, 21, 25, 29
SMT-HC3-C05	c1..c5	1, 5, 9, 13, 17
SMT-HC3-C08	c1..c8	1, 5, 9, 13, 17, 21, 25, 26
PRT-HC3-C16	c1..c16	1, 5, 6, 10, 11, 15, 16, 20, 21, 25, 26, 30, 31, 35, 36, 40

GigaVUE-HC1-Plus

HC1P-C04X08	c1..c4	1, 5, 9, 13
	x1..x8	17..24
PRT-HC1-X12	x1..x12	1..12
PRT-HC1-Q04X08	c1..c4	25, 29, 33, 37

GigaSMART Device / Line Card	Ports	Port IDs Inserted in Gigamon Trailer
	x1..x8	41..48
GigaVUE-HCT		
HCT-C02	c1..c2	1, 5
PRT-HC1-Q04X08	q1..q4	1, 5
	x1..x8	
PRT-HC1-G12	g1..g12	1..12
GigaSMART TA Series		
GigaVUE-TA25	x1..x48	1..48
	c1..c8	49,53,57,61,65,69,73,77
	c1x1..c1x4	49..52
	c5x1..c5x4	65..68
GigaSMART-TA25E	x1..x48	1..48
	c1..c4	49, 53, 57, 61, 65, 69, 73, 77
GigaSMART-TA100	c1..c32	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125
	c1x1..c32x4	1..128
GigaSMART-TA200	c1..c32	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125
	c33..c64	129..160
GigaSMART-TA200E	c1..c32	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125
	c33..c64	1..128
GigaVUE-TA400	d1..d32	129..160
GigaVUE-TA400E	d1..d32	1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 113, 117, 121, 125
	x1..x12	129,130

GigaSMART Trailer Example

The following figures show a sample GigaSMART trailer with the packet length and source ID (Source port label) TLV included. The total length of the trailer in this example is 10 bytes, plus another 5 bytes for the Trailer Length, Ethertype, and Checksum fields.

GIGAMON_PKT_LEN TLV			GIGAMON_SRCID TLV							Trailer Length, Ethertype, Checksum		
GIGAMON_PKT_LEN=1 (1 Byte)	TAG_LEN=2 (2 Bytes)	PKT_LEN=2 (2 Bytes)	GIGAMON_SRCID Type (1 Byte)	GIGAMON_SRCID Length (1 Byte)	Platform (6 Bits)	Group ID (4 Bits)	Box ID (6 Bits)	Slot ID (6 Bits)	Port ID (10 Bits)	Length=10 (0a) (1 Byte)	Ethertype=0x22E5 (2 Bytes)	Checksum (2 Bytes)

← GIGAMON_SRCID Value (4 bytes) →

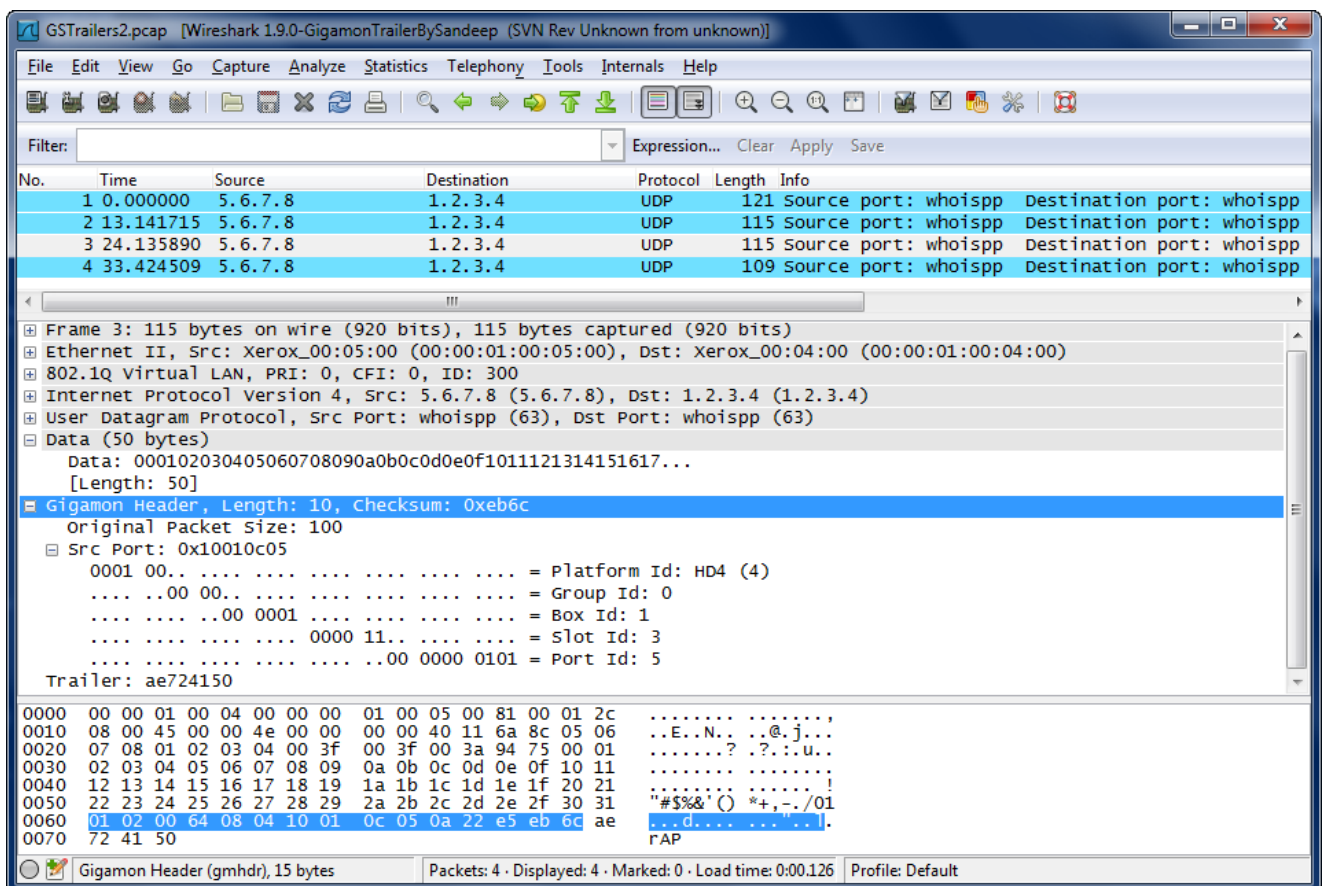


Figure 19 Wireshark Decode of GigaSMART Trailer

Limitations

- Group ID will be set to zero even for the devices in a cluster.
- The Trailer Addition/Removal GSOP does not support E-Tag clusters. GigaVUE-TA400, GigaVUE-TA400E and GigaVUE-HCT platforms support only E-Tag clustering. However, you can configure the GSOP on GigaVUE-HCT platform when operating in standalone mode.
- In Gen2 cards, application chaining, a combination of Trailer Addition with Tunnel Decapsulation, is currently unsupported within the same GSOP. To achieve the intended functionality, you can configure two distinct GSOPs, one for decapsulation and another for trailer addition linked by maps.

GigaSMART Logs

As of 5.4, GS Log files enable you to generate and download application-specific logging information to use for troubleshooting problematic applications. Gigamon Support can use these files for root cause analysis.

GS Log levels are applied at the process level by specifying **info** or *debug* when configuring the logging level for the application's processes. Logging levels modified at the application level will take priority over the system level setting.



To access Logs, click  on the top navigation bar. On the left navigation pane, select **System > Logs**.

Create GS Log file

To create a log file that Gigamon can use for analysis, do the following:

1. Access a device: Physical > Physical Node > click the Cluster ID for a node.
2. Under Support in the navigation pane, select **Debug > GigaSMART Logs**.
3. Click **Generate**.
4. Select the Host Name and Ports.

The screenshot shows the 'GigaSMART Logs - Debug Files' interface. The main area is a table with columns: Host Name, File Name, Status, Eport List, and Completed List. A mouse cursor is hovering over the Host Name column. On the right, there is a sidebar with a 'Generate Debug File' section. This section includes a 'Host Name' dropdown menu with the text 'Select a device' and a 'Ports' dropdown menu with the text 'Select a Ports'. Below these dropdowns is a 'Generate' button.

The system generates a new GS Log file.

5. Select the GS Log file to download, and then click **Download**.

You can only download one file at a time.

The system downloads the file to your local environment with a name like, gsdump_<hostname>_<date>_<time>.tgz.gpg. The file is in a compressed and encrypted format that you can provide to Gigamon.

Delete Log File

To delete the GS Log files for clearing up the disk space:

1. Select **Debug > GS Logs**.
2. Select the GS Logs that you want to delete and click **Delete**.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VÜE Community](#)

Documentation

©This table lists all the guides provided for GigaSMART software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

NOTE: In the online documentation, view [What's New](#) to access quick links to topics for each of the new features in this Release; view [Documentation Downloads](#) to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaSMART 6.14 Hardware and Software Guides	
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing Edit > Advanced Search from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.	
Hardware	how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaSMART devices; reference information and specifications for the respective GigaSMART devices
GigaVUE-HC1 Hardware Installation Guide	
GigaVUE-HC3 Hardware Installation Guide	
GigaVUE-HC1-Plus Hardware Installation Guide	
GigaVUE-HCT Hardware Installation Guide	
GigaVUE-TA25 Hardware Installation Guide	
GigaVUE-TA25E Hardware Installation Guide	
GigaVUE-TA100 Hardware Installation Guide	

GigaSMART 6.14 Hardware and Software Guides	
GigaVUE-TA200 Hardware Installation Guide	
GigaVUE-TA200E Hardware Installation Guide	
GigaVUE-TA400 Hardware Installation Guide	
GigaVUE-TA400E Hardware Installation Guide	
GigaVUE-OS Installation Guide for DELL S4112F-ON	
G-TAP A Series 2 Installation Guide	
GigaVUE M Series Hardware Installation Guide	
GigaVUE-FM Hardware Appliances Guide	
Software Installation and Upgrade Guides	
GigaVUE-FM Installation, Migration, and Upgrade Guide	
GigaVUE-OS Upgrade Guide	
GigaVUE V Series Migration Guide	
Fabric Management and Administration Guides	
GigaVUE Administration Guide	covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
GigaVUE Application Intelligence Solutions Guide	
GigaVUE Inline Solutions Guide(NEW) (previously included in the GigaVUE Fabric Management Guide)	
Cloud Guides	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
GigaVUE V Series Applications Guide	
GigaVUE Cloud Suite Deployment Guide - AWS	
GigaVUE Cloud Suite Deployment Guide - Azure	
GigaVUE Cloud Suite Deployment Guide - OpenStack	
GigaVUE Cloud Suite Deployment Guide - Nutanix	
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)	
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)	

GigaSMART 6.14 Hardware and Software Guides

GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Universal Cloud TAP - Container Deployment Guide

Gigamon Containerized Broker Deployment Guide

GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions

Reference Guides

GigaVUE-OS CLI Reference Guide

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices

GigaVUE-OS Security Hardening Guide

GigaVUE Firewall and Security Guide

GigaVUE Licensing Guide

GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices

Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.

Release Notes

GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;
important notes regarding installing and upgrading to this release

Note: Release Notes are not included in the online documentation.

Note: Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software and Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

In-Product Help

GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to [My Gigamon](#). Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to [My Gigamon](#).
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

NOTE: My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to:

documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

For Online Topics	Online doc link	<i>(URL for where the issue is)</i>
	Topic Heading	<i>(if it's a long topic, please provide the heading of the section where the issue is)</i>
For PDF Topics	Document Title	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings**  **> Support > Contact Support** in GigaVUE-FM.

You can also refer to <https://www.gigamon.com/support-and-services/contact-support> for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives.

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The [VÜE Community](#) is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)