



GigaSMART Subscriber Intelligence Guide

GigaVUE-FM, GigaVUE HC Series

Product Version: 6.14.02

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
6.14.02	2.0	09/07/2026	Increased GigaStream scale for Subscriber Intelligence load balancing. Refer to Required License: GTP Filtering and CUPS Correlation
6.14	1.0	02/07/2026	The original release of this document with 6.14.00 GA.

Contents

GigaSMART Subscriber Intelligence Guide	1
Change Notes	3
Contents	4
GigaSMART-Subscriber-Intelligence	8
Subscriber Intelligence	8
Prerequisite	15
Site	16
cpNode	16
upNode	16
5GPolicy	16
LTEPolicy	16
Deployment of Non-CUPS Solution	16
Required License: GTP Filtering and CUPS Correlation	17
Entire session sampling for Mobile subscribers	46
Dynamic Session Sampling for Fixed Wireless Access Subscribers	47
Sampling Window	47
Enabling Dynamic Sampling	47
Session Handling	48
Offset Configuration	48
Required License:	54
Required Licenses: SIP/RTP Correlation (and FlowVUE for session-aware load balancing for RTP)	55
Example: Tool port 1/1/x1 is configured with a threshold of 3k pps.	63
SIP/RTP Load Balancing Example	64
SIP/RTP Minimum Configuration Example	64
Configure ports	65
Create Virtual Ports	66
Configure GigaSMART Operation	67
Create first level map	68
Create second level map for SIP Flow Sampling.	69
Create the SIP whitelist	70
Associate the GigaSMART group to the SIP whitelist.	70
Configure GigaSMART operation for SIP whitelisting	70
Configure first level map	71
Create another second level map for SIP flow whitelist	71
Required License: FlowVUE	72

FlowVUE Configuration Examples	73
Display FlowVUE Statistics	73
Required Licenses: GTP Filtering & Correlation and FlowVUE	80
PFCP Messages	119
About Standalone UPN Flow Sampling Map Mode and Port Groups	125
Standalone Configuration	125
Cluster Configuration	126
Standalone UPN Flow Sampling Map Priority	127
Virtual Port Configuration in Standalone UPN Mode	127
PFCP Messages	128
About Standalone UPN Flow Sampling Map Mode and Port Groups	134
Standalone Configuration	134
Cluster Configuration	135
Standalone UPN Flow Sampling Map Priority	136
Virtual Port Configuration in Standalone UPN Mode	136
Interface Filtering	137
APN (Access Point Name)/DNN (Data Network Name) Filtering	138
Custom Interface Selection	139
Supported Platforms:	140
Required License : 5G-Correlation and CUPS	142
Supported Platforms	144
Configure 5G Load Balancing	145
5G RAN Correlation	146
Configure 5G RAN Correlation	147
5G Network Slice Correlation	147
Configure 5G Network Slice Correlation	149
5QI Correlation	149
Rules and Notes	149
Required License : FlowVUE license is required for Flow Sampling	149
About Flow Sampling Rules and Maps	150
Configure GTP Overlap Mapping	153
Configuration Considerations	153
Standalone Configuration	153
Cluster Configuration	155
Overlap Map Statistics	162
5G Stateful Session Recovery	163
Required License: 5G Correlation	163
Configure 5G Stateful Session Recovery	163
View Backup and Restore information	164
Remove Backup files	166
Required License : 5G Whitelisting	166

Configure Whitelist Maps	167
Change Priority of Whitelist Maps	168
Delete Whitelist Maps	168
Rules and Notes	170
Configure Stand-Alone User Plane Node Traffic Monitoring	170
Creating Inventory Directory	173
Creating fmInfo.yml	173
Creating ansible_inputs.json	173
Creating 3G/4G control plane metadata inventory file	173
Creating host_vars directory	176
Creating host_vars files	177
Prerequisite	177
Site	178
cpNode	178
upNode	178
5GPolicy	178
LTEPolicy	178
Deployment of 3G/4G Control Plane Metadata Solution	178
Set up of additional variable for Single GigaVUE-FM instance	178
Execute the Playbook	178
Creating Inventory Directory	179
Creating fmInfo.yml	179
Creating ansible_inputs.json	179
Creating 5G control plane metadata inventory file	180
Creating host_vars directory	182
Creating host_vars files	183
Prerequisite	183
Site	184
cpNode	184
upNode	184
5GPolicy	184
LTEPolicy	184
Deployment of 3G/4G Control Plane Metadata Solution	184
Set up of additional variable for Single GigaVUE-FM instance	184
Execute the Playbook	184
Configure CPN-UPN Communication using Ansible	187
Configure CPN-UPN Communication using CLI	188
Create Inventory Directory	188
Create fmInfo.yml	189
Create ansible_inputs.json File	189
Create an Inventory File for CPN-UPN Communication	189
Create host_vars directory	190
Create host_vars files	190

Deploy CPN-UPN Communication Solution in Ansible	196
View CPN-UPN Communication Solution in GigaVUE-FM,GigaVUE HC Series	197
Remove CPN-UPN Communication	198
Flow Sample Map Rules for CPN-UPN Communication	198
Rules and Notes:	198
Forward List Map Rules for CPN-UPN Communication	200
Rules and Notes:	200
Configuration Considerations	221
Standalone Configuration	222
Cluster Configuration	223
This section contains:	226
Example 1: GTP Overlap Mode	226
Required License: GTP Filtering & Correlation	232
Required License: GTP Filtering & Correlation	235
Required License: GTP Filtering & Correlation	236
Passing GTP Control Traffic	236
Display Statistics	238
How to Download Software and Release Notes from My Gigamon	250
Premium Support	253
Glossary	254

GigaSMART-Subscriber-Intelligence

Subscriber Intelligence

Designed to meet the needs of service providers, these GigaSMART operations provide complete network and subscriber visibility to increase the efficiency of network monitoring, security, and customer experience tools.

NOTE: GigaSMART mobility is not supported in GigaVUE-HCT devices.

Subscriber Intelligence	
GTP Correlation	▪ Required License: GTP Filtering and CUPS Correlation ▪ Required License: ▪ Required Licenses: GTP Filtering & Correlation and FlowVUE ▪ Display Flow Ops Reports ▪ Configuration Considerations ▪ Required License: GTP Filtering & Correlation ▪ Required License: GTP Filtering & Correlation
SIP/RTP Correlation	▪ Required Licenses: SIP/RTP Correlation (and FlowVUE for session-aware load balancing for RTP)
FlowVUE	▪ Required License: FlowVUE
5G CUPS	• Configure 5G Load Balancing • 5G Flow Sampling and Filtering • Required License : FlowVUE license is required for Flow Sampling • Rules and Notes • Create Inventory Directory

Installation and Configuration of Subscriber Intelligence Solution using Ansible

The Gigamon Ansible Module consists of various playbooks that converts high level user intent in YAML format into JSON format.

The GigaVUE-FM uses the JSON format and translates the inputs into various individual components like GigaSMART GSgroups, GSOPs, FlowMaps, etc that are configured on the Physical or Virtual devices.

The Gigamon Ansible Module exposes playbooks that allows the configuration and maintenance of the Subscriber Intelligence solutions and the GigaVUE-FM GUI allows you to visualise, monitor and troubleshoot Subscriber Intelligence Solutions.

Refer to the following sections for configuring the Subscriber Intelligence solution:

- [System Requirements](#)

- [Installation and Configuration of Gigamon Ansible Module](#)
- [Rules and Notes](#)

The Gigamon Ansible Module allows you to configure the following:

S.No	Steps	Refer to..
1.	CUPS Solution	Configure CPN-UPN Communication Solution using Ansible
2.	Non-CUPS Solution	Configuration of Non-CUPS using Ansible

System Requirements

Ensure that the following environment is available before installing 'gigamon-ansible':

- **Python version:** 2.7.15 or greater
- **Operating System:** Linux
- **Ansible version:** 2.9.4 or greater
- **Python Packages**
 - **requests** - Install this using *pip install requests*
 - **ruamel.yaml** -Install this using *ruamel.yaml*
 - **jsonschema** - Install this using *pip install jsonschema*
 - **netaddr** - Install this using *pip install netaddr*

Installation and Configuration of Gigamon Ansible Module

Gigamon-Ansible module can be installed as follows:

Package	Operating System	Commands to install the Package
RPM package	CentOS	<code>sudo yum install <packageName>.rpm</code>
Deb package	Ubuntu	<code>sudo apt install <packageName>.deb</code>

The package is extracted under the path */usr/local/share/gigamon*.

For setting the Pythonpath, add the following to *~/.bashrc* and source it:

```
export INSTALL_DIR=/usr/local/share/gigamon
export PYTHONPATH=$PYTHONPATH:$INSTALL_DIR
```

Deployment Report

Everytime a Subscriber Intelligence solution is deployed/updated/deleted, a deployment report is generated in the path declared in the **ansible_inputs.json** file.

Check Mode

The checkmode feature allows you to find the difference between the configuration that is already present in the GigaVUE-FM against the payload that you are trying to apply without applying the new payload in GigaVUE-FM. This allows you to quickly find the components that gets affected if the new configuration is applied.

The check mode can be enabled by adding **--check** to the command that triggers the playbook.

```
/usr/bin/ansible-playbook --check -e '@~/cupsSolution/ansible_inputs.json' -i  
~/cupsSolution/cups_inventory /usr/local/share/gigamon-ansible/playbooks/cups/deploy_  
cups.yml
```

The output of **--check** is a Deployment Report that contains the difference in configuration as shown:

Deployment Report Checkmode

```
Deployment_Report_Checkmode  
deploymentPayloadDiff:  
  updated:  
    - path: //trafficPolicies/LTE/whitelisting/flowMaps/wlMapInternetToEEA/rules/rule_1/interface  
      old_value: S11  
      new_value: s11  
    - path: //trafficPolicies/LTE/whitelisting/flowMaps/wlMapGeoProbe/rules/rule_1/apn  
      old_value: apn.airtel.com  
      new_value: apn.vodafone.com  
  removed: []  
  created: []  
deploymentRequest: EDIT  
deploymentResponse: CHECK MODE  
timeStamp: 09-Mar-2020::12:12:1583781162
```

Reapplying Golden Payload

It is also possible to restore the configuration from the generated Golden Payload file using one of the following two commands:

- `/usr/bin/ansible-playbook -e '@~/mobilitySolution/ansible_inputs.json' -e 'applyGP=True' -i ~/mobilitySolution/mobility_inventory /usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_mobility_solution.yml`
- `/usr/bin/ansible-playbook -e '@~/mobilitySolution/ansible_inputs.json' -e 'applyGP=True' --ask-vault-pass -i ~/mobilitySolution/mobility_inventory /usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_mobility_solution.yml`

It is also possible to enable checkmode to find the difference between the configuration on GigaVUE-FM and the configuration of the Golden Payload. The command to do is:

- `/usr/bin/ansible-playbook --check -e '@~/mobilitySolution/ansible_inputs.json' -e 'applyGP=True' -i ~/mobilitySolution/mobility_inventory /usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_mobility_solution.yml`
- `/usr/bin/ansible-playbook --check -e '@~/mobilitySolution/ansible_inputs.json' -e 'applyGP=True' --ask-vault-pass -i ~/mobilitySolution/mobility_inventory /usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_mobility_solution.yml`

NOTE: It searches the golden payload file to reapply the configuration in the default location if the file path is not defined in the **ansible_inputs.json** file.

Rules and Notes

You must ensure the following rules and notes while deploying Subscriber Intelligence Solution:

- GigaVUE-FM, GigaVUE HC Series is reachable from the server on which Ansible is executed.
- All the required licenses are installed on the Gigamon devices.
- The required permission for RBAC is available.
- Configurations that are not handled by the Mobility playbook are pre-configured.
- Migration of Subscriber Intelligence Solution from GigaVUE-FM 5.9 to any other version is impossible.

Configuration of Non-CUPS using Ansible

To configure a Non-CUPS solution, perform the following steps:

S.No	Steps	Refer to..
1.	Creating Inventory Directory	Creating Inventory Directory
2.	Creating <i>fmInfo.yml</i>	Creating fmInfo.yml
3.	Creating <i>ansible_inputs.json</i>	Creating ansible_inputs.json
4.	Creating Non-CUPS inventory file	Creating Non-CUPS inventory file
5.	Creating host_vars directory	Creating host_vars directory
6.	Creating host_vars files	Creating host_vars files

Creating Inventory Directory

Create an *Inventory Directory* to store all the Non-CUPS related configuration files.

```
username@fmreg26:~$ mkdir non-CupsSolution
username@fmreg26:~$ ls -l
drwxr-xr-x 2 ddaniel fmtaf 4096 May 11 11:59 non-CupsSolution
```

Creating *fmInfo.yml*

Create *fmInfo.yml* file inside the Inventory Directory that contains the information such as ip-address, username and password.

To create the file, refer to [Schema](#).

Creating *ansible_inputs.json*

Create '*ansible_inputs.json*' file inside the Inventory Directory.

- ```
gigamon@fmreg26:~/non-cupsSolution$ ls -l
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

*File name: ansible\_inputs.json*

To create a file, refer to [Schema](#).

## Creating Non-CUPS inventory file

Create the *mobility\_inventory* file inside Inventory Directory.

```
gigamon@fmreg26:~/nonCupsSolution$ touch mobility_inventory

gigamon@fmreg26:~/nonCupsSolution$ ls -l
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
-rw-r--r-- 1 gigamon fmtaf 396 May 11 14:22 mobility_inventory
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

The file contains the details of the following groups and provide the inputs to the groups as shown in the following table:

| S.No                                                                                                                                      | Groups-Input                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Note:</b> –You can provide the input or leave the field empty if you don't want to use the playbook to configure the following groups. |                                                                                                               |
| 1.                                                                                                                                        | <b>Ports</b> –Name of the Cluster or standalone device IP that contains the ports that need to be configured. |

| S.No | Groups-Input                                                                                                                     |
|------|----------------------------------------------------------------------------------------------------------------------------------|
| 2.   | <b>IPInterfaceSolution</b> —Name of the Cluster or standalone device IP on which the IPInterfacesolution needs to be configured. |
| 3.   | <b>Tool Groups</b> —Name of the Cluster or standalone device IP on which the ToolGroup needs to be configured.                   |
| 4.   | <b>GigaStreams</b> —Name of the Cluster or standalone device IP on which the Gigastreams needs to be configured.                 |
| 5.   | <b>GTPWhitelist</b> —Name of the Cluster or standalone device IP on which the GTPWhitelist Data Base needs to be configured.     |
| 6.   | <b>Policies</b> —Name of the Global policy or policies.                                                                          |
| 7.   | <b>GTP</b> — Name of the GTP node or nodes.                                                                                      |
| 6.   | <b>CPN</b> —Name of the CPN or CPNs.                                                                                             |
| 7.   | <b>UPN</b> —Name of the UPN or UPNs.                                                                                             |
| 8.   | <b>SAM</b> —Name of SAMs Exporter node or nodes.                                                                                 |
| 9.   | <b>Sites</b> —Name of the site or sites and the names of the CPN/UPN participating in the site or sites.                         |
| 10.  | <b>CUPS</b> —Name of the file containing information of the solution level RBAC Tags.                                            |

*File name: mobility\_inventory (Single GigaVUE-FM instance)*

```
[IPInterfaceSolution]

[ToolGroups]
cluster-two
cluster-one

[Gigastreams]
cluster-two
cluster-one

[GTPWhitelist]
cluster-two
cluster-one

[Ports]
cluster-two
cluster-one

[Policies]
5g_policy_1

[GTP]
gtp_CorrelationNode1

[CPN]

[UPN]

[SAM]
```

```
[Sites]
UK cpn_list='["cpnUKLTE"]' upn_list='[]' sam_list='[]'
Dallas cpn_list='[]' upn_list='["upnDallas"]' sam_list='[]'

[MobilitySolution]
mobilitySolution1 cups_5g_global_policy=5g_policy_1 sites='["UK", "Dallas"]'
```

*File name: cups\_inventory (Multiple GigaVUE-FM instances)*

```
[IPInterfaceSolution]

[ToolGroups]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Gigastreams]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[GTPWhitelist]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Ports]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Policies]
5g_policy_1

[GTP]
gtp_CorrelationNode1

[CPN]

[UPN]

[SAM]

[Sites]
UK cpn_list='["cpnUKLTE"]' upn_list='[]' sam_list='[]'
Dallas cpn_list='[]' upn_list='["upnDallas"]' sam_list='[]'

[MobilitySolution]
mobilitySolution1 cups_5g_global_policy=5g_policy_1 sites='["UK"]' fm_ip=192.168.36.2
mobilitySolution2 cups_5g_global_policy=5g_policy_1 sites='["Dallas"]' fm_ip=192.168.36.3
```

## Creating **host\_vars** directory

Create **host\_vars** directory inside the Inventory Directory.

```
gigamon@fmreg26:~/nonCupsSolution$ mkdir host_vars

gigamon@fmreg26:~/nonCupsSolution$ ls -l
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
-rw-r--r-- 1 gigamon fmtaf 396 May 11 14:22 cups_inventory
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
drwxr-xr-x 2 gigamon fmtaf 4096 May 11 14:48 host_vars
```

## Creating **host\_vars** files

Every unique element under each group in the *mobility\_inventory* file needs to have a file, with the same name as the element, inside **host\_vars** directory. This file has properties of the groups that it belongs to.

Below are the templates of various **host\_vars** files.

## Prerequisite

```

validate_certs: false
Ports:
- port:
 - 1/1/x1
 - 1/1/x2
 adminStatus: enable
 type: network

GTPWhitelist:
- alias: gtp1
 imsi: 310260564627811,310260564627812
 state: present
- alias: gtp2
 inputFile: './whitelistKeys/TenIMSIValid.txt'
 state: present

Gigastreams:
- alias: toolGS_C11
 ports:
 - 4/1/x1
 - 4/1/x2
 type: hybrid
 state: present
- alias: toolGS_C12
 ports:
 - 4/1/x3..x4
```

```
type: hybrid
state: present

ToolGroups:
- alias: pgGrp_C11
 ports:
 - 2/1/x1
 smartLb: false
 type: tool
 state: present
- alias: pgGrp_C12
 ports:
 - 2/1/x2
 smartLb: false
 type: tool
 state: present
```

## Site

For information about **Site**, refer to [Schema](#).

## cpNode

For information about **cpNode**, refer to [Schema](#).

## upNode

For information about **upNode**, refer to [Schema](#).

## 5GPolicy

For information about **5GPolicy**, refer to [Schema](#).

## LTEPolicy

For information about **LTEPolicy**, refer to [Schema](#).

# Deployment of Non-CUPS Solution

To deploy the Non-CUPS solution, follow these steps:

## Set up of additional variable for Single GigaVUE-FM instance

For a Single GigaVUE-FM instance deployment, you must set an additional environment variable as follows.

```
export ANSIBLE_FM_IP=192.168.36.2
```

It searches the login details of the GigaVUE-FM IP in *fmInfo.yml* file.

## Execute the Playbook

- You can execute the playbook and deploy the CUPS solution using the following command:

```
/usr/bin/ansible-playbook -e '@~/cupsSolution/ansible_inputs.json' -i
~/cupsSolution/cups_inventory /usr/local/share/gigamon-ansible/playbooks/cups/deploy_
cups.yml
```

- If the *fmInfo* file is encrypted, use the following command to execute and deploy CUPS solution:

```
/usr/bin/ansible-playbook -e '@~/cupsSolution/ansible_inputs.json' --ask-vault-pass -i
~/cupsSolution/cups_inventory /usr/local/share/gigamon-ansible/playbooks/cups/deploy_
cups.yml
```

**NOTE:** The multiple YML files created inside the **host\_vars** are concatenated, converted into JSON format and sent to GigaVUE-FM.

## GigaSMART GTP and CUPS Correlation

Required License: GTP Filtering and CUPS Correlation

Supported Devices: GigaVUE-HC3 Gen 2

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

The GigaSMART GTP application correlates traffic based on mobile subscriber IDs in the packet data networks of service providers. It provides a mechanism to filter and forward session traffic for subscribers to tools. GTP and CUPS correlation assists mobile carriers in debugging and analyzing GTP traffic in their 3G/4G networks.

**NOTE:** For Generation 3 cards, you can use Flow Sampling with sampling rate as 100% to achieve the same behavior as flow filtering.

- GPRS Tunneling Protocol (GTP) is an IP/UDP-based protocol that carries mobile data across service provider networks. The protocol is used in General Packet Radio Service (GPRS) networks such as: Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), and Long Term Evolution (LTE). The protocol encapsulates user data that passes through the core network and carries subscriber-specific signaling traffic.

- GTP includes both control plane (GTP-c) and user-data plane (GTP-u) traffic. To gain an accurate view into the subscriber's session, GTP tunnels are used to correlate the subscriber-specific control plane and user-data plane traffic. A GTP session is the minimum unit of GTP and CUPS correlation consisting of one control and multiple user tunnels. All GTP traffic belonging to the same session is forwarded to the same tool port.
- Using GTP and CUPS correlation, you can filter, replicate, and forward specific subscriber sessions to specific tools by correlating the subscriber IDs that are exchanged as part of the control sessions to the corresponding tunnel IDs (TEIDs) that are part of the user-data plane traffic.

GTP and CUPS correlation provides the following:

- stateful filtering based on subscriber IDs (IMSI, IMEI, and MSISDN)
- stateful filtering based on GTP version or EPC interface
- stateful correlation of GTP-c with GTP-u traffic
- correlation of subscriber ID with corresponding tunnel ID
- forwarding of the subscriber-specific control and user-data plane traffic to a tool or group of tools
- It supports 12 million GTP subscriber sessions for GigaVUE-HC3 nodes.
- In Subscriber Intelligence deployments that use GigaSMART GTP and CUPS correlation with stateful load balancing, a load-balanced port group (LBPG) whose members are GigaStreams can now include up to 64 GigaStream members on GigaSMART Gen3 C08 line cards.
- option to combine with GigaSMART Load Balancing to load balance GTP traffic to a set of tool ports. For information on GTP load balancing, refer to stateful load balancing in the section [GigaSMART Load Balancing](#). For examples of GTP load balancing, refer to [GTP Correlation Configuration Examples](#). Starting in software version 4.6, GTP load balancing in a cluster is supported for GTP flow filtering. For an example of GTP load balancing in a cluster, refer to [GTP Whitelisting and GTP Flow Sampling Examples](#).

Starting in software version 4.5, a GigaSMART group (gsgroup) associated with GTP applications can have multiple GigaSMART engine port members (e ports), up to four, forming an engine group. Refer to [GTP Scaling](#).

## Licensing Requirements

- For GTP flow sample with the rule percentage (0 or 100), the **GTP\_MAX** license is required.
- For GTP flow sample with the rule percentage in all ranges (between 0 to 100) or for GTP Whitelist, the **GTP\_MAX** and **FVUE** licenses are required
- For GTP flow filtering, the **GTP\_MAX** license is required. The GTP flow filtering is supported only on Gen 2 devices.

### Filtering on Subscriber IDs and Version

GTP stateful filtering supports filtering of GTP sessions based on the following subscriber IDs:

| Component | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| imsi      | <p>The International Mobile Subscriber Identity (IMSI) is a number that identifies a subscriber of a cellular network. It is a unique identification associated with all cellular networks.</p> <p>An IMSI is usually a 15 digit number, associated with GSM, UMTS, and LTE network mobile phone users.</p>                                                                                                                                                                  |
| imei      | <p>The International Mobile Station Equipment Identity (IMEI) is a number, usually unique, that identifies 3rd Generation Partnership Project (3GPP), for example, GPRS, LTE, as well as Integrated Digital Enhanced Network (iDEN) mobile phones, and some satellite phones.</p> <p>The IMEI identifies the device, but has no permanent relationship to the subscriber. Instead, the subscriber is identified by transmission of an IMSI number, stored on a SIM card.</p> |
| msisdn    | <p>The Mobile Station International Subscriber Directory Number (MSISDN) is a unique number that identifies subscribers in a GSM or UMTS mobile network. This numbering plan is defined in the ITU-T recommendation E.164. The maximum length of an MSISDN is 15 digits.</p>                                                                                                                                                                                                 |

In addition to filtering on subscriber IDs, you can optionally filter on GTP version (v1 or v2) or Evolved Packet Core (EPC) interface. Filtering on the EPC interface allows traffic to be segmented for a given interface.

The supported interfaces for EPC filtering are as follows:

- Gn/Gp
- S11U
- S11/S1-U
- S5/S8
- S10
- S2B

**NOTE:** When GigaSMART receives S5 and S11 GTP-C control traffic that share the same control TEID, and an S5 is received very close in time to the S5 Create Session Response, GigaSMART may retain only one of the S5 or S11 endpoints in the mobility statistics. The other endpoint might not be visible in whitelist map statistics or Flow-Ops reports.

When filtering on EPC interface, you do not also need to specify version, as the version is implied.

To create maps using GTP, specify a **Second Level Flow Sample** map and select **GTP** for the rule. When adding a map rule, you can specify the following:

- subscriber IDs (IMSI, IMEI, or MSISDN)
- number of digits. The maximum number of digits for the IMSI or MSISDN value is 15. The maximum number of digits for the IMEI value is 16. To specify the prefix for IMSI, IMEI, or MSISDN, you can use a wild card character or a digit string followed by a wild card character.
- map comment to label the purpose of a rule or the type of traffic covered by a rule

- GTP version 1 or version 2 (refer to [Figure 1GTP Version](#)) or EPC interface Gn/GP, S5/S8, or S10, S2B, or S11/S1U (refer to [Figure 2GTP EPC Interface](#))

**NOTE:** In a map, version and EPC interface cannot be specified in the same flowrule, but they can be specified in different flowrules.

**NOTE:** The maximum number of GTP flowrules is 32 per map.

For examples of filtering on GTP version, refer to [Required License: GTP Filtering and CUPS Correlation](#).

Map Rules

Add a Rule

Rule 1 Condition search...

**GTP**

Priority: 1 Percentage: %

IMEI: IMEI

IMSI: IMSI

MSISDN: MSISDN

QCI: 0-255

APN: APN

Version -- -- Any V1 V2

Map Order

Figure 1 GTP Version

Map Rules

Add a Rule

**x Rule 1** Condition search...

**GTP**

Priority: 1 Percentage: %

IMEI: IMEI

IMSI: IMSI

MSISDN: MSISDN

QCI: 0-255

APN: APN

Interface --

- 
- Gn/Gp
- S5/S8**
- S10
- S11/S1U

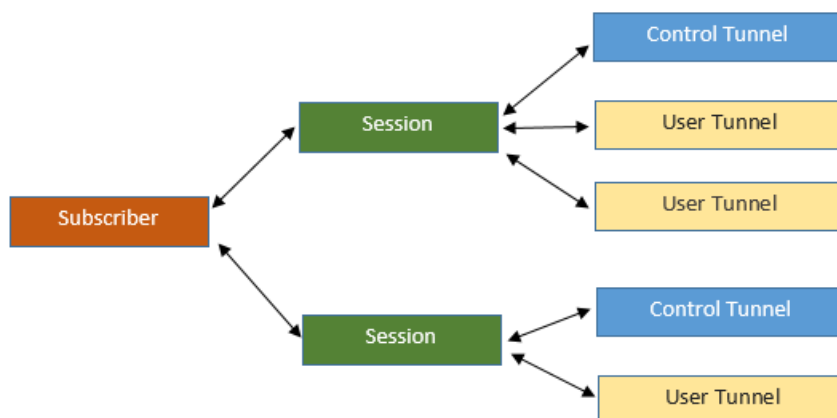
Map Order

Priority

Figure 2 GTP EPC Interface

### Session Correlation

Each GTP session has one control tunnel and one or more user tunnels. All the tunnels are correlated together into a session. Packets belonging to the same session will be forwarded to the same tool port. Refer to the following figure.



In a second level map, the following can be specified:

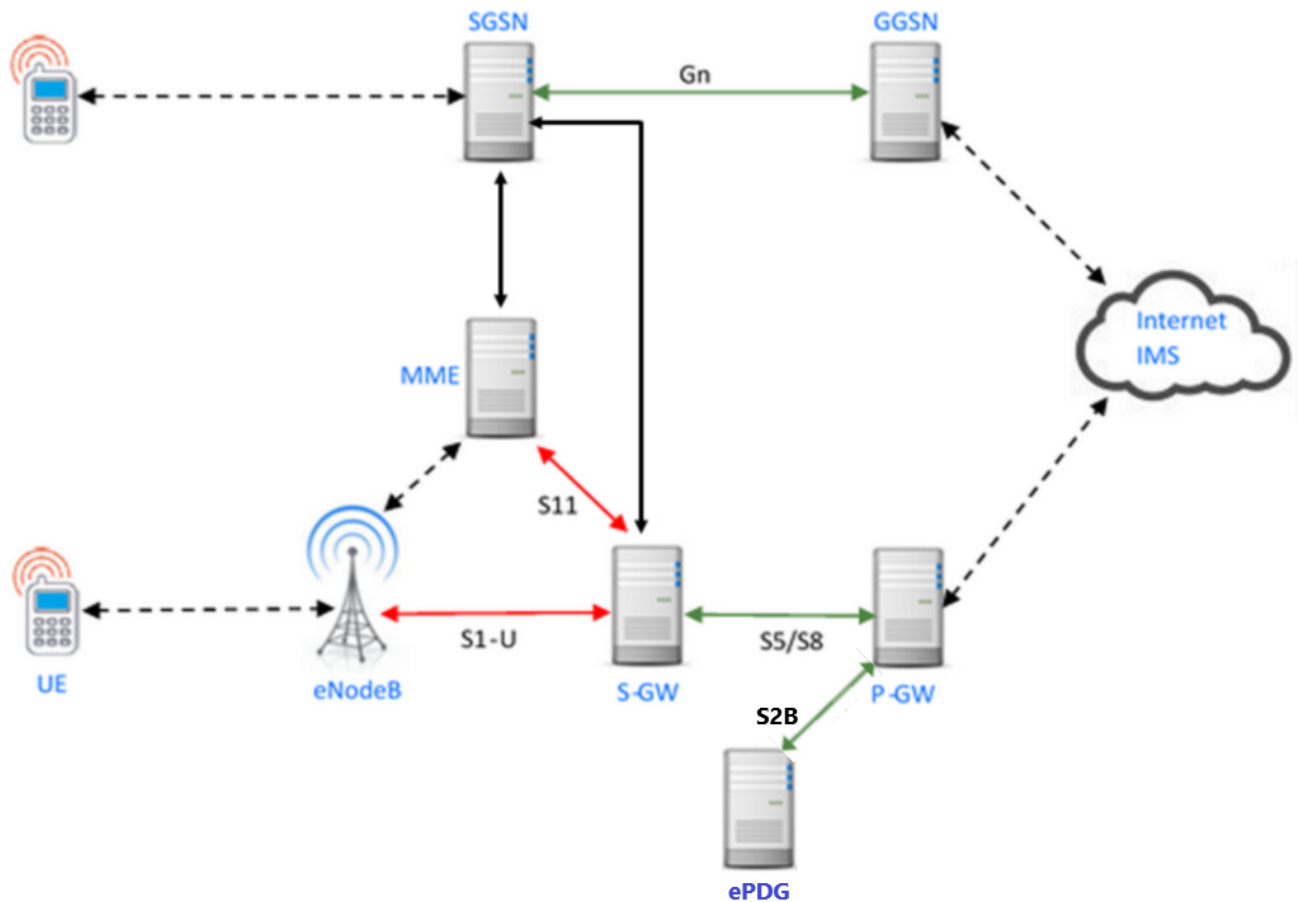
- one tool port—packets from one subscriber (same subscriber ID), from one or more GTP sessions, will be forwarded to the same tool port.
- multiple tool ports—packets from one subscriber (same subscriber ID), from multiple GTP sessions will be correlated and forwarded to same tool port. Using load balancing, GTP traffic that matches the same map but belongs to different subscribers can be load balanced to multiple tool ports.

#### Supported Interfaces

GTP is used at multiple interfaces by multiple devices in the core network. GTP stateful correlation is implemented for the following interfaces:

- Gn/Gp (for GPRS). The Gn interface is between SGSN-GGSN only.
- S5/S8 (for LTE)
- S1-U, S11U and S11 (for LTE)
- S10 (for S1-based mobility) Refer to [Conditional S10 Support](#)
- S2B

Support for interfaces for both GPRS and LTE networks includes the handovers between the different networks. Refer to the following figure.



For LTE networks, the following GTP traffic will be correlated to the specific mobile subscriber and routed to the same tool port:

- GTP-c traffic on the S11 interface between MME and S-GW
- GTP-u traffic on the S11u interface between MME and S-GW
- GTP-u traffic on the S1u interface between eNodeB and S-GW
- GTP-c traffic on the S10 interface between MMEs
- GTP-c traffic on the S5/S8 interface between S-GW and P-GW
- GTP-u traffic on the S5u interface between S-GW and P-GW
- GTP-c traffic on the S2b interface between P-GW and ePDG
- GTP-u traffic on the S2b-U interface between P-GW and ePDG

In order to correlate GTP-c and GTP-u traffic running on different interfaces, you must tap into the correct interfaces, as follows:

- Gn/Gp—one interface runs both GTP-c and GTP-u
- S5/S8—one interface runs both GTP-c and GTP-u
- S1u, S11u, and S11—these three interfaces have to be tapped at the same time to get both GTP-c and GTP-u to perform the correct correlation.

- S2b-C and S2b-U interfaces needs to be tapped to get GTP-c and GTP-u traffic for correlation.

For examples of filtering on GTP interface types Gn/Gp, S5/S8, S1 and S11, refer to [Required License: GTP Filtering and CUPS Correlation](#).

#### Conditional S10 Support

The following table outlines support for the S10 interface. In the table, No means not supported, Conditional means there is limited support of the S10 interface.

| S10                                          | Support                                                                                                                          |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Forward Relocation Request/Resp              | Conditional; IMSI must be present in Forward Relocation Request                                                                  |
| Forward Relocation Complete Notification/Ack | Conditional; IMSI must be present in Forward Relocation Request for Forward Relocation Complete Notification/Ack to be supported |
| Context Request/Response and Ac              | Conditional; IMSI must be present                                                                                                |
| Identification Request/Response              | No                                                                                                                               |
| Forward Access Context Notification/Ack      | No                                                                                                                               |
| Relocation Cancel Request/Response           | No                                                                                                                               |
| Configuration Transfer Tunnel                | No                                                                                                                               |

#### GTP Session Timeout

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.

In prior software versions, the complete GTP session timeout was eight hours. Starting with software version 4.2, the GTP session timeout is configurable, with eight hours as the default.

To configure the GTP session timeout, do the following:

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Groups > GigaSMART Groups**.
2. Click **New** to create a new GigaSMART Group or **Edit** to modify an existing one.
3. Under GigaSMART Parameters, go to GTP Flow.
4. Enter the timeout in the **Timeout** field. The following figure shows an example where the timeout value is set to 60.

▼ GTP Flow

5. Click **Save**.

The GTP session timeout disconnects a GTP session if it has been inactive for the timeout value. The timeout can be configured as an integer from 1 to 6000, in increments of 10 minutes. The default value is 48, which is 480 minutes, which is 8 hours.

## Priorities for Flow Rules and Maps

One virtual port can have multiple maps, and for each map, you can add multiple flow rules with different filtering attributes. The priorities for flow rules are as follows:

- a rule with a drop action has a higher priority than a rule with a pass action
- for the same pass or drop action, the priorities are IMSI, IMEI, or MSISDN in descending order

In a GTP session, if one IMSI, IMEI, or MSISDN rule is matched, the map is matched. For example, if any one of the following matches any rule shown in the following figure, map1 (which is a Second Level Flow Filter map) is matched:

Map Rules

Add a Rule

x Rule 1

☒ Pass ☐ Drop

GTP IMSI

x

1234\*

Version

Any

x Rule 2

☒ Pass ☐ Drop

GTP IMEI

x

467\*

Version

Any

x Rule 3

☒ Pass ☐ Drop

GTP MSISDN

x

32332\*

Version

Any

In addition, in one map, all drop rules are matched first and all pass rules are matched next.

For example, in a GTP session, if an IMSI matches the first rule in map1 and an IMEI matches the second rule in map1, because the drop rule has higher priority, the packet will be dropped:

▼ Map Rules

Add a Rule

✕ Rule 1  ☒ Pass ☐ Drop

**GTP IMSI** ✕

1234\* Version ▼ Any ▼

✕ Rule 2  ☐ Pass ☒ Drop

**GTP IMEI** ✕

467\* Version ▼ Any ▼

If multiple maps are matched, the map with the highest priority will be considered for further processing. For example, the [Figure 3 Rule in Map1](#) shows the rule for map1 while the rule [NetFlow Generation Gigamon Solution](#) shows the rule for map2. In a GTP session, if an IMSI matches the first rule in map1 and an IMEI matches the first rule in map2, because map1 has higher priority, the packet will be passed.

▼ Map Rules

Add a Rule

✕ Rule 1  ☒ Pass ☐ Drop

**GTP IMSI** ✕

1234\* Version ▼ Any ▼

**Figure 3** Rule in Map1

Figure 4 Rule in Map2

### GTP Correlation Configuration Examples

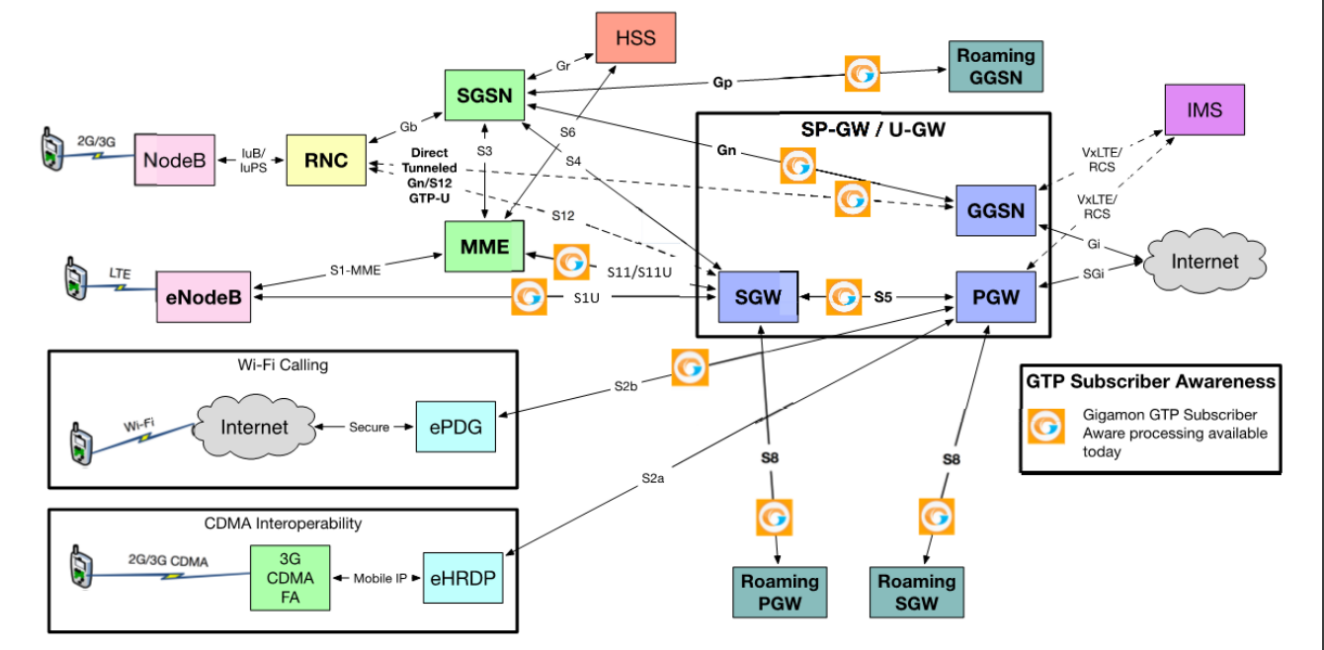
The following sections provide examples of GTP correlation and GTP load balancing. Refer to the following examples:

- [Example 1: Identifying High-Value and/or Roaming Subscribers Based on IMSIs](#)
- [Example 2: Identifying GTP Versions](#)
- [Example 3: Same Subscriber, Filter on Different Versions](#)
- [Example 4: Same Subscriber, Filter on Different Interfaces](#)
- [Example 5: EPC Filtering in Scenario1](#)
- [Example 6: EPC Filtering in Scenario2](#)

### Example 1: Identifying High-Value and/or Roaming Subscribers Based on IMSIs

Use GTP correlation to identify high value subscribers based on an IMSI or group of IMSIs. GTP correlation keeps track of the IMSIs that you are interested in monitoring. It correlates them to the corresponding data/user-plane sessions for the subscriber and/or group of subscribers. Filtering on subscriber ID (IMSI) limits the amount of traffic that is sent to monitoring tools.

# LTE EPC Network - 3G/4G/LTE



In Example 1, filter rules are configured to identify and forward all the traffic related to subscribers identified by an IMSI prefix. All traffic specific to the filtered IMSIs 2222222222223\*, including GTP-c and GTP-u, is forwarded to a monitoring tool. A shared collector is configured to which traffic not matching the filters is sent.

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.

| Task | Description                                                          | UI Steps                                                                                                                                                                                                                                                                                                                     |
|------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                    | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports.</li> <li>2. Click Quick Port Editor.</li> <li>3. In the Quick View Editor set one port to Network and two ports to Tool.</li> <li>4. Select Enable on each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol> |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> </ol>                                                                                                                                                           |

| Task | Description                                                                                                                                                                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | port.                                                                                                                                                                                                                          | <ol style="list-style-type: none"> <li>Click New.</li> <li>Type a name for the GigaSMART Group in the Alias field.</li> <li>Click in the Port List field and select an engine port.</li> <li>Under GTP Flow set the Timeout. The default is value is 48, which is 480 minutes.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group to enable GTP correlation.                                                                                                                              | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP &gt; GigaSMART Operation</b>.</li> <li>Type a name for the GigaSMART Group in the Alias field.</li> <li>Click in the GigaSMART Operations (GSOP) field and select Flow Filtering.</li> <li>Click OK.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                |
| 4    | Configure a virtual port and assign it to the same GigaSMART group.                                                                                                                                                            | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</li> <li>Click New.</li> <li>Type a name for the virtual port in the Alias field.</li> <li>Click in the GigaSMART Groups field, and select the GigaSMART Group created in Task 2.</li> <li>Click OK.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                        |
| 5    | <p>Create a first level map that directs GTP traffic from physical network port/s to the virtual port you created in the previous step.</p> <p><b>Note:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.</p> | <ol style="list-style-type: none"> <li>Select Maps &gt; Maps &gt; Maps</li> <li>Click New.</li> <li>Configure the map. <ul style="list-style-type: none"> <li>Enter an alias</li> <li>Select First Level for Type</li> <li>Select By Rule for Subtype</li> <li>Select a network port for the Source</li> <li>Select the virtual port configured in Task 4 for the Destination</li> </ul> </li> <li>Create Rule 1. <ol style="list-style-type: none"> <li>Click Add a Rule</li> <li>Select Pass.</li> <li>Select Bi Directional.</li> <li>Select Port Source</li> <li>Set the source to 2123</li> </ol> </li> <li>Create Rule 2. <ol style="list-style-type: none"> <li>Click Add Rule</li> <li>Select Pass.</li> </ol> </li> </ol> |

| Task | Description                                                                                                                                                                                       | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>c. Select Bi Directional</li> <li>d. Select Port Source</li> <li>e. Set the source to 2152</li> </ul> <ol style="list-style-type: none"> <li>6. Create Rule 3. <ul style="list-style-type: none"> <li>a. Click Add Rule</li> <li>b. Select Pass.</li> <li>c. Select IPv4 Fragmentation</li> <li>d. Set Value to allFragNoFirst</li> </ul> </li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                 |
| 6    | Create a second level map that takes traffic from the virtual port, applies the GigaSMART operation, matches IMSIs specified by the flow rule, and sends matching traffic to physical tool ports. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Filter for Subtype</li> <li>■ Select the virtual port configured in Task for the Source</li> <li>■ Select the tool port configured in Task 1 for the Destination</li> <li>■ Select the GigaSMART Operation created in Task 3 from the GSOP list.</li> </ul> </li> <li>4. Create a rule. <ul style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select GTP IMSI.</li> <li>d. Enter 22222222222223* in the IMSI field.</li> </ul> </li> <li>5. Click Save.</li> </ol> |
| 7    | Add a shared collector for any unmatched data and send it to the second tool port.                                                                                                                | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias</li> <li>■ Select Second Level for Type</li> <li>■ Select Collector for Subtype</li> <li>■ Select a the virtual port configured in Task for the Source</li> <li>■ Select the second tool port configured in Task 1 for the Destination</li> </ul> </li> <li>4. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                        |
| 8    | Display the configuration for Example 1.                                                                                                                                                          | To display the configuration for the GigaSMART Group:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Task | Description | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups</b>.</li> <li>2. Click on the alias for the GigaSMART Group to display the Quick View.</li> </ol> <p>To display the configuration for the GigaSMART Operation:</p> <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP) &gt; GigaSMART Operation</b>.</li> <li>2. Click on the alias for the GigaSMART Operation to display the Quick View.</li> </ol> <p>To display the configuration for the maps:</p> <ol style="list-style-type: none"> <li>1. Select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>2. Click on a map alias to display the Quick View for the map.</li> </ol> |

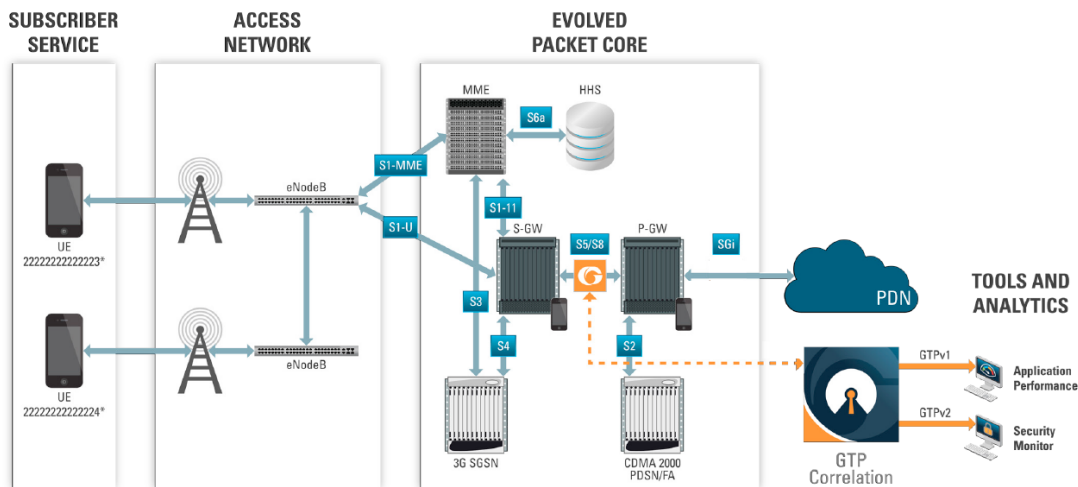
## Display GTP Correlation Flow Ops Report Statistics

To display GTP correlation statistics associated with the GigaSMART group, select **GigaSMART > GigaSMART Operations > Statistics**.

Refer to [Flow Ops Report Statistics Definitions for GTP on page 635](#) for descriptions of these statistics.

## Example 2: Identifying GTP Versions

As part of GTP correlation, GigaVUE-FM, GigaVUE HC Series nodes also provide the flexibility to identify GTPv1 and GTPv2 messages. GTP version information is typically exchanged only as part of the control sessions. By correlating the control and user-plane sessions, GigaVUE-FM, GigaVUE HC Series nodes can identify, filter, and forward all sessions specific to a GTPv1 or v2 to one or more monitoring/analytic tools.



In Example 2, EMEI traffic is distributed based on GTP versions as follows:

- Filter and forward GTPv1 to a tool port
- Filter and forward GTPv2 to another tool port

| Task | Description                                                                                       | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                                                 | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports.</li> <li>2. Click Quick Port Editor.</li> <li>3. In the Quick View Editor set one port to Network and two ports to Tool.</li> <li>4. Select Enable on each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                             |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port.                        | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field.</li> <li>4. Click in the Port List field and select an engine port.</li> <li>5. Under GTP Flow set the Timeout. The default is value is 48, which is 480 minutes.</li> <li>6. Click Save.</li> </ol> |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group to enable GTP correlation. | <ol style="list-style-type: none"> <li>1. From the device view, select <b>GigaSMART &gt; GigaSMART Operations &gt; GigaSMART Operation</b>.</li> <li>2. Type a name for the GigaSMART Group in the Alias field.</li> <li>3. Click in the GigaSMART Operations (GSOP) field and select Flow Filtering.</li> <li>4. Click Save.</li> </ol>                                                                                                                 |

| Task | Description                                                                                                                                                                                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4    | Configure a virtual port and assign it to the same GigaSMART group.                                                                                                                                                                        | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; Virtual Ports</b>.</li> <li>2. Click New.</li> <li>3. Type a name for the virtual port in the Alias field.</li> <li>4. Click in the GigaSMART Groups field, and select the GigaSMART Group created in Task 2.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 5    | <p>Create a first level map that directs GTP traffic from physical network ports to the virtual port you created in the previous task.</p> <div> <p><b>NOTE:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.</p> </div> | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>o Enter an alias</li> <li>o Select First Level for Type</li> <li>o Select By Rule for Subtype</li> <li>o Select a network port for the Source</li> <li>o Select the virtual port configured in Task 4 for the Destination</li> </ul> </li> <li>4. Create Rule 1. <ol style="list-style-type: none"> <li>a. Click Add a Rule</li> <li>b. Select Pass.</li> <li>c. Select Bi Directional.</li> <li>d. Select Port Source</li> <li>e. Set the source to 2123</li> </ol> </li> <li>6. Create Rule 2. <ol style="list-style-type: none"> <li>a. Click Add Rule</li> <li>b. Select Pass.</li> <li>c. Select Bi Directional</li> <li>d. Select Port Source</li> <li>e. Set the source to 2153</li> </ol> </li> <li>6. Create Rule 3. <ol style="list-style-type: none"> <li>a. Click Add Rule</li> <li>b. Select Pass.</li> <li>c. Select IPv4 Fragmentation</li> <li>d. Set Value to allFragNoFirst</li> </ol> </li> <li>5. Click Save.</li> </ol> |
| 6    | Create a second level map that takes traffic from the virtual port, applies the GigaSMART operation, matches IMEIs specified by the flow rule, and sends matching traffic to a tool port.                                                  | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>o Enter an alias</li> <li>o Select Second Level for Type</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Task | Description                                                                                                                                                                                     | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>o Select Flow Filter for Subtype</li> <li>o Select a the virtual port configured in Task for the Source</li> <li>o Select the a tool port configured in Task 1 for the Destination</li> <li>o Select the GigaSMART Operation created in Task 3 from the GSOP list.</li> </ul> <ol style="list-style-type: none"> <li>4. Create a rule.               <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select GTP IMSI.</li> <li>d. Enter * in the IMSEI field and set Version to V1</li> </ol> </li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                         |
| 7    | Create a second level map that takes traffic from the virtual port, applies the GigaSMART operation, matches IMEIs specified by the flow rule, and sends matching traffic to another tool port. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map.               <ul style="list-style-type: none"> <li>o Enter an alias</li> <li>o Select Second Level for Type</li> <li>o Select Flow Filter for Subtype</li> <li>o Select a the virtual port configured in Task for the Source</li> <li>o Select the second tool port configured in Task 1 for the Destination</li> <li>o Select the GigaSMART Operation created in Task 3 from the GSOP list.</li> </ul> </li> <li>4. Create a rule.               <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select GTP IMSEI.</li> <li>d. Enter * in the IMSI field and set Version to V2</li> </ol> </li> <li>5. Click Save.</li> </ol> |
| 8    | Display the configuration for Example 2.                                                                                                                                                        | <p>To display the configuration for the GigaSMART Group:</p> <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; Maps.</li> <li>2. Click on the alias for the GigaSMART Group to display the Quick View.</li> </ol> <p>To display the configuration for the GigaSMART Group:</p> <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operations</li> <li>2. Click on the alias for the GigaSMART Operation to display the Quick View.</li> </ol> <p>To display the configuration for the maps:</p>                                                                                                                                                                           |

| Task | Description | UI Steps                                                                                                                                                        |
|------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click on the map alias to display the Quick View for the map.</li> </ol> |

### Example 3: Same Subscriber, Filter on Different Versions

In this example, traffic from the same subscriber is forwarded to two different load balancing groups based on version. GTP version 1 traffic is sent to one load balancing group and GTP version 2 traffic is sent to another load balancing group.

| Task | Description                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and multiple tool type of ports.                     | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports.</li> <li>2. Click Quick Port Editor.</li> <li>3. In the Quick View Editor set one port to Network and multiple ports to Tool. For example, set 1/2/g1 as a Network port and ports 1/2/g5 through 1/2/g9 as Tool ports.</li> <li>4. Select Enable on each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                                            |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port. | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field.</li> <li>4. Click in the Port List field and select an engine port.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                             |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group.    | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations &gt; GigaSMART Operations</b>.</li> <li>2. Type a name for the GigaSMART Group in the Alias field.</li> <li>3. Click in the GigaSMART Operations field and select Flow Filtering.</li> <li>4. Click in the GigaSMART Operations filed and select Load Balancing.</li> <li>5. Configure the Load Balancing as follows: <ul style="list-style-type: none"> <li>o Select Stateful</li> <li>o Select GTP for Type</li> </ul> </li> </ol> |

| Task | Description                                                                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                | <ul style="list-style-type: none"> <li>o Selecting Hashing</li> <li>o Select IMSI</li> </ul> <ol style="list-style-type: none"> <li>6. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 4    | Configure a virtual port and assign it to the GigaSMART group.                                                                 | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; Virtual Ports</b>.</li> <li>2. Click New.</li> <li>3. Type a name for the virtual port in the Alias field.</li> <li>4. Click in the GigaSMART Groups field, and select the GigaSMART Group created in Task 2.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                           |
| 5    | Create two port groups (one for version 1 traffic and one for version 2 traffic) and enable load balancing on the port groups. | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Port Groups &gt; All Port Groups.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field. For example, pglbv1.</li> <li>4. Select SMART Load Balancing to enable load balancing</li> <li>5. Click in the Ports field and select half the tool ports configured in Task 1.</li> <li>6. Repeat steps 2 through 4, creating a second port group with the other ports configured in Task 1</li> </ol>                                                                                                                                                                                                                                                        |
| 6    | Create an ingress (first level) map.                                                                                           | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>o Enter an alias. For example, map1_1.</li> <li>o Select First Level for Type</li> <li>o Select By Rule for Subtype</li> <li>o Select a network port for the Source</li> <li>o Select the virtual port configured in Task 4 for the Destination</li> </ul> </li> <li>4. Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>o Select pass</li> <li>o Select MAC Destination</li> <li>o Enter a MAC address. For example, <b>00:a0:d1:e1:02:01</b></li> <li>o Enter a MAC mask. For example, 0000.0000.0000</li> </ul> </li> <li>5. Click Save.</li> </ol> |
| 7    | Create a second level map for version1.                                                                                        | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>o Enter an alias. For example, map2_1.</li> <li>o Select Second Level for Type</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Task | Description                                   | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                               | <ul style="list-style-type: none"> <li>o Select Flow Filter for Subtype</li> <li>o Select the virtual port configured in Task 4 for the Source</li> <li>o Select the first port group for Destination</li> <li>o Select the GigaSMART Operation configured in Task 3 from the GSOP list.</li> </ul> <ol style="list-style-type: none"> <li>4. Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>o Select Pass</li> <li>o Select GTP IMSI</li> <li>o Enter * in the IMSI field</li> <li>o Select <b>V1</b> for Version</li> </ul> </li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                              |
| 8    | Create another second level map for version2. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>o Enter an alias. For example, map2_2.</li> <li>o Select Second Level for Type</li> <li>o Select Flow Filter for Subtype</li> <li>o Select the virtual port configured in Task 4 for the Source</li> <li>o Select the second port group for Destination</li> <li>o Select the GigaSMART Operation configured in Task 3 from the GSOP list.</li> </ul> </li> <li>4. Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>o Select Pass</li> <li>o Select GTP IMSI</li> <li>o Enter * in the IMSI field</li> <li>o Select <b>V2</b> for Version</li> </ul> </li> <li>5. Click Save.</li> </ol> |

### Example 4: Same Subscriber, Filter on Different Interfaces

In this example, traffic from the same subscriber is forwarded to two different load balancing groups based on interface. In this example, VLANs 1601 and 1602 are from S5/S8 interface and VLANs 1611 and 1612 are from S11/S1-U interface. The first level maps split the VLAN traffic to different virtual ports. The second level maps send the traffic to different load balancing groups.

| Task | Description                                                                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and multiple tool type of ports.                                                                         | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports.</li> <li>2. Click Quick Port Editor.</li> <li>3. In the Quick View Editor set one port to Network and multiple ports to Tool. For example, set 1/2/g1 as a Network port and ports 1/2/g5 through 1/2/g9 as Tool ports.</li> <li>4. Select Enable on each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                                                                                          |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port.                                                     | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field.</li> <li>4. Click in the Port List field and select an engine port.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                     |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group.                                                        | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Operations &gt; GigaSMART Operations.</li> <li>2. Type a name for the GigaSMART Group in the Alias field.</li> <li>3. Click in the GigaSMART Operations field and select Flow Filtering.</li> <li>4. Click in the GigaSMART Operations field and select Load Balancing.</li> <li>5. Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Select GTP for Type</li> <li>■ Selecting Hashing</li> <li>■ Select IMSI</li> </ul> </li> <li>6. Click Save.</li> </ol> |
| 4    | Configure virtual ports and associate them with the GigaSMART group.                                                           | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; Virtual Ports.</li> <li>2. Click New.</li> <li>3. Type a name for the virtual port in the Alias field.</li> <li>4. Click in the GigaSMART Groups field, and select the GigaSMART Group created in Task 2.</li> <li>5. Click Save.</li> <li>6. Repeat steps 1 through 5 to create a second virtual port.</li> </ol>                                                                                                                                                                                                            |
| 5    | Repeat task 4 to create another virtual port.                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 6    | Create two port groups (one for version 1 traffic and one for version 2 traffic) and enable load balancing on the port groups. | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Port Groups &gt; All Port Groups.</li> <li>2. Click New.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Task | Description                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                            | <ol style="list-style-type: none"> <li>3. Type a name for the GigaSMART Group in the Alias field. For example, pglbv1.</li> <li>4. Select SMART Load Balancing to enable load balancing</li> <li>5. Click in the Ports field and select half the tool ports configured in Task 1.</li> <li>6. Repeat steps 2 through 4, creating a second port group with the other ports configured in Task 1</li> </ol>                                                                                                                                                                                                                                                                                           |
| 7    | Create a first level map for vport1.       | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias. For example, map1_1.</li> <li>■ Select First Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Select a network port for the Source</li> <li>■ Select the first virtual port configured in Task 4 for the Destination</li> </ul> </li> <li>4. Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>■ Select Pass</li> <li>■ Select VLAN</li> <li>■ Enter 1601 for the Min value</li> <li>■ Enter 1602 for the Max value</li> </ul> </li> <li>5. Click Save.</li> </ol> |
| 8    | Create another first level map for vport2. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias. For example, map1_2.</li> <li>■ Select First Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Select a network port for the Source</li> <li>■ Select the second virtual port configured in Task 5 for the Destination</li> </ul> </li> <li>4. Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>■ Select Pass</li> <li>■ Select VLAN</li> <li>■ Enter 1611 for the Min value</li> <li>■ Enter 1611 for the Max value</li> </ul> </li> </ol>                        |

| Task | Description                                   | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                               | <ol style="list-style-type: none"> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 9    | Create a second level map using vport1.       | <ol style="list-style-type: none"> <li>Select Maps &gt; Maps &gt; Maps.</li> <li>Click New.</li> <li>Configure the map. <ul style="list-style-type: none"> <li>Enter an alias. For example, map2_1.</li> <li>Select Second Level for Type</li> <li>Select Flow Filter for Subtype</li> <li>Select the virtual port configured in Task 4 for the Source</li> <li>Select the first port group for Destination</li> <li>Select the GigaSMART Operation configured in Task 3 from the GSOP list.</li> </ul> </li> <li>Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>Select Pass</li> <li>Select GTP IMSI</li> <li>Enter * in the IMSI field</li> </ul> </li> <li>Click Save.</li> </ol>         |
| 10   | Create another second level map using vport2. | <ol style="list-style-type: none"> <li>Select Maps &gt; Maps &gt; Maps.</li> <li>Click New.</li> <li>Configure the map. <ul style="list-style-type: none"> <li>Enter an alias. For example, map2_2.</li> <li>Select Second Level for Type</li> <li>Select Flow Filter for Subtype</li> <li>Select the second virtual port configured in Task 5 for the Source</li> <li>Select the second port group for Destination</li> <li>Select the GigaSMART Operation configured in Task 3 from the GSOP list.</li> </ul> </li> <li>Click Add a Rule to create a rule. <ul style="list-style-type: none"> <li>Select Pass</li> <li>Select GTP IMSI</li> <li>Enter * in the IMSI field</li> </ul> </li> <li>Click Save.</li> </ol> |

## Example 5: EPC Filtering in Scenario1

In this example, traffic for all subscribers on interfaces S11/S1-U and Gn/Gp is sent to the same load balancing group. All other traffic is dropped.

| Task | Description                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                          | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports.</li> <li>2. Click Quick Port Editor.</li> <li>3. In the Quick View Editor set one port to Network and two ports to Tool. For example, set 1/2/g1 as a Network port and ports 1/2/g5 and 1/2/g6 as Tool ports.</li> <li>4. Select Enable on each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                                                                                                                    |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port. | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field.</li> <li>4. Click in the Port List field and select an engine port.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                      |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group.    | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>2. Type a name for the GigaSMART Group in the Alias field.</li> <li>3. Click in the GigaSMART Operations field and select Flow Filtering.</li> <li>4. Click in the GigaSMART Operations (GSOP) field and select Load Balancing.</li> <li>5. Configure the Load Balancing as follows. <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Select GTP for Type</li> <li>■ Selecting Hashing</li> <li>■ Select IMSI</li> </ul> </li> <li>6. Click Save.</li> </ol> |
| 4    | Configure a virtual port and assign it to the GigaSMART group.             | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; Virtual Ports.</li> <li>2. Click New.</li> <li>3. Type a name for the virtual port in the Alias field.</li> <li>4. Click in the GigaSMART Groups field, and select the GigaSMART Group created in Task 2.</li> </ol>                                                                                                                                                                                                                                                                                                                           |

| Task | Description                                                                                                                                                                                        | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                    | <ol style="list-style-type: none"> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5    | Create a port group enable load balancing on the port group.                                                                                                                                       | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Port Groups &gt; All Port Groups.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field. For example, pglbv1.</li> <li>4. Select SMART Load Balancing to enable load balancing</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 6    | <p>Create an ingress (first level) map.</p> <p><b>Note:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.</p>                                                                     | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias</li> <li>■ Select First Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Select a network port for the Source</li> <li>■ Select the virtual port configured in Task 4 for the Destination</li> </ul> </li> <li>4. Create Rule 1. <ol style="list-style-type: none"> <li>a. Click Add a Rule</li> <li>b. Select Pass.</li> <li>c. Select Bi Directional.</li> <li>d. Select Port Source</li> <li>e. Set the source to 2123</li> </ol> </li> <li>6. Create Rule 2. <ol style="list-style-type: none"> <li>a. Click Add Rule</li> <li>b. Select Pass.</li> <li>c. Select Bi Directional</li> <li>d. Select Port Source</li> <li>e. Set the source to 2152</li> </ol> </li> <li>6. Click Save.</li> </ol> |
| 7    | Create a second level map that takes traffic from the virtual port, applies the GigaSMART operation, matches IMSIs specified by the flow rules, and sends matching traffic to physical tool ports. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias.</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Filter for Subtype</li> <li>■ Select the virtual port configured in Task 4 for the Source</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Task | Description | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | <ul style="list-style-type: none"> <li>■ Select the port group for Destination</li> <li>■ Select the GigaSMART Operation configured in Task 3 from the GSOP list.</li> </ul> <ol style="list-style-type: none"> <li>4. Create the rule 1.               <ol style="list-style-type: none"> <li>a. Click Add a Rule</li> <li>b. Select Pass</li> <li>c. Select GTP IMSI</li> <li>d. Enter * in the IMSI field</li> <li>e. Select Interface and set it to Gg/Gp</li> </ol> </li> <li>6. Create rule 2.               <ol style="list-style-type: none"> <li>a. Click Add a Rule</li> <li>b. Select Pass</li> <li>c. Select GTP IMSI</li> <li>d. Enter * in the IMSI field</li> <li>e. Select Interface and set it to S11/S1U</li> </ol> </li> <li>6. Click Save.</li> </ol> |

## Example 6: EPC Filtering in Scenario2

In this example, traffic for all subscribers from all interfaces except S5/S8 is sent to the same load balancing group. Traffic from the S5/S8 interface is dropped.

| Step | Description                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                          | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports.</li> <li>2. Click Quick Port Editor.</li> <li>3. In the Quick View Editor set one port to Network and two ports to Tool. For example, set 1/2/g1 as a Network port and ports 1/2/g5 and 1/2/g6 as Tool ports.</li> <li>4. Select Enable on each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol> |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port. | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field.</li> <li>4. Click in the Port List field and select an engine port.</li> </ol>                                                                                                           |

| Step | Description                                                                                                         | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                     | <ol style="list-style-type: none"> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group.                                             | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>2. Type a name for the GigaSMART Group in the Alias field.</li> <li>3. Click in the GigaSMART Operations (GSOP) field and select Flow Filtering.</li> <li>4. Click in the GigaSMART Operations (GSOP) field and select Load Balancing.</li> <li>5. Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Select GTP for Type</li> <li>■ Selecting Hashing</li> <li>■ Select IMSI</li> </ul> </li> <li>6. Click Save.</li> </ol> |
| 4    | Configure a virtual port and assign it to the GigaSMART group.                                                      | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; Virtual Ports.</li> <li>2. Click New.</li> <li>3. Type a name for the virtual port in the Alias field.</li> <li>4. Click in the GigaSMART Groups field, and select the GigaSMART Group created in Task 2.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                      |
| 5    | Create a port group and enable load balancing on the port group.                                                    | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Port Groups &gt; All Port Groups.</li> <li>2. Click New.</li> <li>3. Type a name for the GigaSMART Group in the Alias field. For example, pglbv1.</li> <li>4. Select SMART Load Balancing to enable load balancing</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                       |
| 6    | Create an ingress (first level) map.<br><b>Note:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias</li> <li>■ Select First Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Select a network port for the Source</li> <li>■ Select the virtual port configured in Task 4 for the Destination</li> </ul> </li> <li>4. Create Rule 1. <ol style="list-style-type: none"> <li>a. Click Add a Rule</li> </ol> </li> </ol>                                                                                                               |

| Step | Description                                                                                                                                                                                        | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>b. Select Pass.</li> <li>c. Select Bi Directional.</li> <li>d. Select Port Source</li> <li>e. Set the source to 2123</li> </ul> <p>6. Create Rule 2.</p> <ul style="list-style-type: none"> <li>a. Click Add Rule</li> <li>b. Select Pass.</li> <li>c. Select Bi Directional</li> <li>d. Select Port Source</li> <li>e. Set the source to 2152</li> </ul> <p>6. Click Save.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 7    | Create a second level map that takes traffic from the virtual port, applies the GigaSMART operation, matches IMSIs specified by the flow rules, and sends matching traffic to physical tool ports. | <ul style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Enter an alias.</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Filter for Subtype</li> <li>■ Select the virtual port configured in Task 4 for the Source</li> <li>■ Select the port group for Destination</li> <li>■ Select the GigaSMART Operation configured in Task 3 from the GSOP list.</li> </ul> </li> <li>4. Create the rule 1. <ul style="list-style-type: none"> <li>a. Click Add a Rule</li> <li>b. Select drop</li> <li>c. Select GTP IMSI</li> <li>d. Enter * in the IMSI field</li> <li>e. Select Interface and set it to S5/S8</li> </ul> </li> <li>6. Create rule 2. <ul style="list-style-type: none"> <li>a. Click Add a Rule</li> <li>b. Select Pass</li> <li>c. Select GTP IMSI</li> <li>d. Enter * in the IMSI field</li> </ul> </li> <li>5. Click Save.</li> </ul> |

## GigaSMART Rotational Sampling

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

Rotational Sampling samples sessions by International Mobile Subscriber ID (IMSI), using a rotating or sliding IMSI range, that rotates automatically on a configurable interval, without disrupting the treatment of existing sessions. It rotates through the entire pool of subscribers over time, such that all subscribers can be sampled in.

The IMSI range size is configurable, the length of time for each period or window is configurable, and as is the length of time for each period or window. Additionally, the amount it shifts or slides every period is also configurable.

This capability supports both network security and performance monitoring. Sampling should account for all active subscribers and be deterministic, so it is always evident whether a subscriber is included.

In Rotational Sampling, the pool of IMSIs is updated at regular intervals, ensuring that all subscribers have an opportunity to participate in the sampling.

Rotational Sampling is now enhanced to support two configuration options -

1. Entire Session Sampling for Mobile Subscribers
2. Dynamic Session Sampling for Fixed Wireless Access Subscribers.

### Entire session sampling for Mobile subscribers

The rotations do not disrupt treatment of existing sessions. Entire sessions are sampled in or out based upon the occurrence of the **"Create Session Requests in GTP-C"** or **"Session Establishment Requests in PFCP"**. Once a session is sampled in, it will remain sampled in for the life of the session, even if the session's IMSI later rotates out of the sampling range.

If the subscriber does not have any create session activity during their rotation window, then nothing will be forwarded for that subscriber in that round. The following parameters are considered while configuring an Entire Session Sampling for Mobile Subscribers:

- **Interval:** Defines how often the sampling window shifts. For example, an interval of 60 means the eligible IMSI range changes every 60 minutes.
- **Sample:** Specifies the size of the IMSI range (in percentage) that is selected for session sampling during each interval. For example, a sample of 30% means 30% of IMSIs are eligible within the active window.
- **Offset:** Determines how much the starting point of the IMSI sampling range shifts at every interval. The offset spreads IMSIs more evenly across intervals. For example, with an offset of 10%, the window moves forward by 10% of the IMSI range each time the interval changes.

The following diagram illustrates an example of an Entire Session Sampling for Mobile Subscribers:

## Entire Session Sampling for Mobile Subscribers

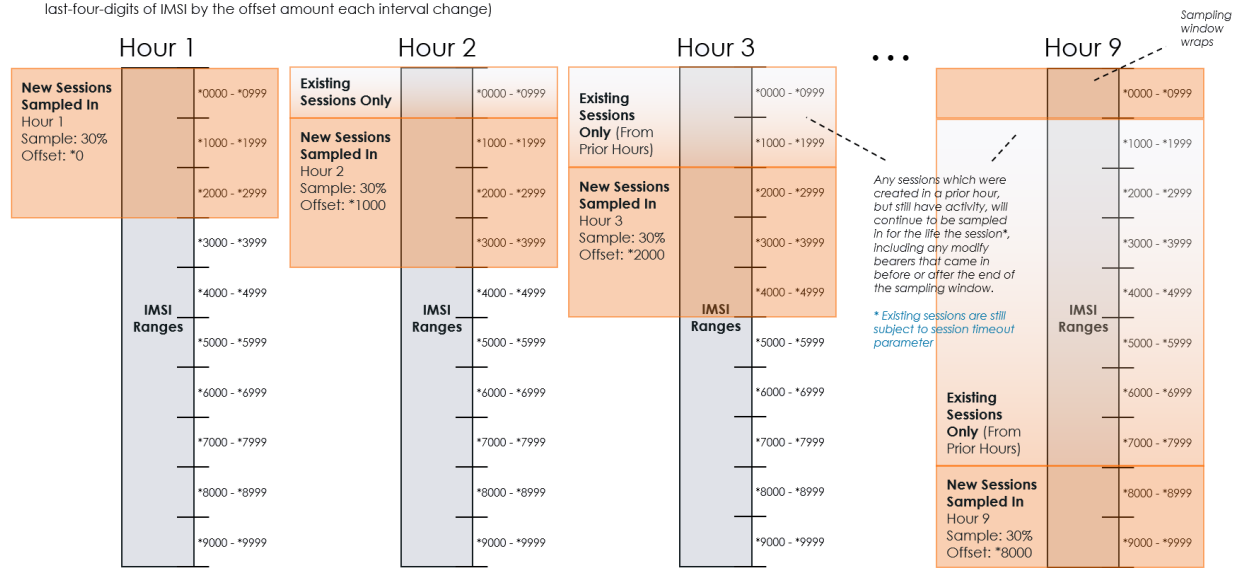
**Example 1: 30% sample, rotation shifts every 1 hour, sliding on 10% of IMSIs**

Parameters:

- Interval = 60** (Shift in the window happens every 60 minutes)
- Sample = 30%** (Size of the sampling range)
- Offset = 10%** (Amount to shift the starting point of the sampling range each interval. Offset shifts the last-four-digits of IMSI by the offset amount each interval change)

**In this example:**

- Every 10 hours, every IMSI is eligible for sampling
- Each IMSI's eligible sampling window lasts for a consecutive 3 hours
- Over 4 days, each IMSI will also have been eligible for sampling-in for every wall-clock hour of the day



## Dynamic Session Sampling for Fixed Wireless Access Subscribers

Dynamic Session Sampling enables the system to periodically re-evaluate which subscriber sessions are actively being sampled. This feature is specifically designed for Fixed Wireless Access subscribers, as their sessions often last for extended periods and could otherwise remain sampled indefinitely.

### Sampling Window

The subscriber IMSIs are divided into sampling windows, which rotate at configurable intervals (for example, every 12 hours). Only sessions with IMSIs in the current window are eligible for sampling. For Home Internet FWA subscribers, a 12-hour rotation is recommended to maintain balance and coverage. This approach prevents the same IMSIs from being repeatedly sampled and ensures broader data diversity.

### Enabling Dynamic Sampling

Dynamic Sampling is controlled through a map rule flag called *Periodic Recalculation*.

- When enabled:** It re-evaluates all ongoing sessions at each rotation. If a session's IMSI no longer qualifies for the current window, that session is excluded until its IMSI re-enters a future window.
- When disabled:** Once a session is accepted, it stays sampled until the session ends, following the traditional "whole-session" sampling behavior.

This flexibility allows operators to choose between continuous fairness (enabled) or stable, session-based sampling (disabled).

## Session Handling

At the end of every sampling interval, the system rotates the active IMSI window. A map lookup is performed for ongoing sessions whenever control or user packets are received. Only sessions that match the current IMSI window and the *Periodic Recalculation* setting continue to be sampled, while the rest are excluded until they fall into a later window. This ensures that only sessions aligned with the latest sampling policy remain active.

## Offset Configuration

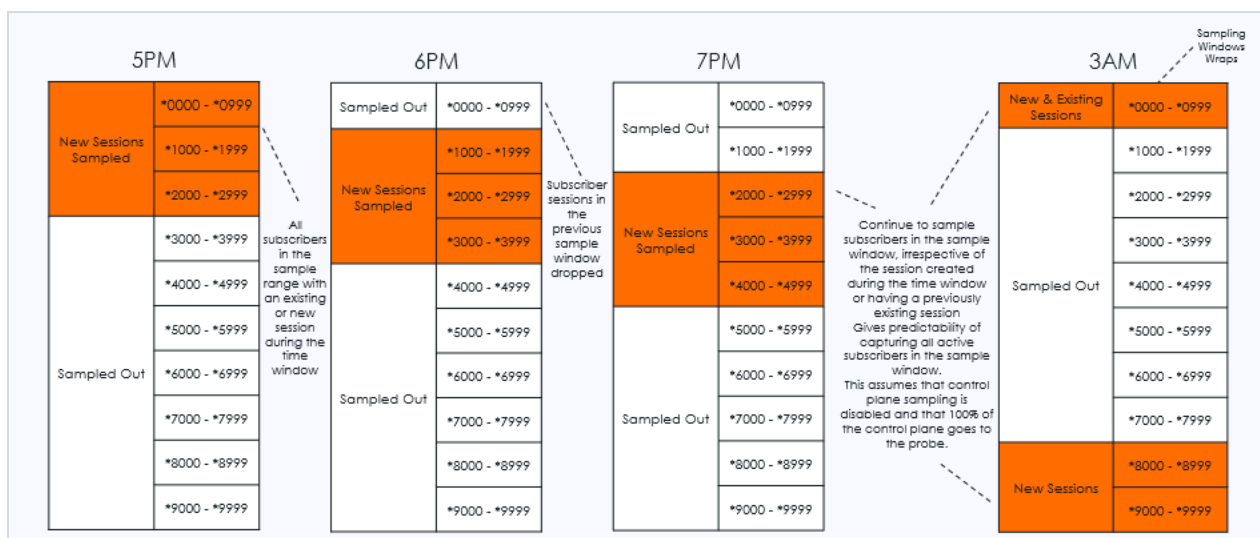
It is recommended to configure the offset value less than the sampling percentage to ensure even distribution of IMSI with maximum correlation. When the offset is less than the sampling percentage, each IMSI is sampled multiple times across different intervals, preventing missed or over-sampled entries. This overlap creates a rolling window effect that smooths out the sampling distribution and helps avoid gaps in the data.

Conversely, if the offset is equal to or greater than the sampling percentage, some IMSIs may be skipped or sampled too infrequently.

For example, with a 25% sampling percentage and a 25% offset, each IMSI would only be sampled once every four intervals, leading to potential data gaps.

**NOTE:** It is advisable to disable GTP-control sampling during the configuration of Dynamic Session Sampling.

The following diagram illustrates an example of Dynamic Session Sampling:



## Supported Platforms Compatibility

The Rotational Sampling feature is supports Entire session sampling for Mobile Subscribers in Non-CUPS LTE ( Non-CUPS GTP application) and UPN (Non-Overlap and Overlap). The table below outlines the supported compatibility.

| Platforms              | Non-CUPS      |         | UPN           |         |
|------------------------|---------------|---------|---------------|---------|
|                        | Non - Overlap | Overlap | Non - Overlap | Overlap |
| GigaVUE-HC3 Gen 3      | ✓             | ✓       | ✓             | ✓       |
| GigaVUE-HC3 Gen 2      | ✓             | ✗       | ✗             | ✗       |
| GigaVUE-HC1-Plus Front | ✓             | ✓       | ✗             | ✗       |
| GigaVUE-HC1-Plus Rear  | ✓             | ✓       | ✗             | ✗       |

The Rotational Sampling feature supports Dynamic session sampling for Fixed Wireless Access Subscribers in Non-CUPS LTE ( Non-CUPS GTP application) and UPN (Non-Overlap and Overlap). The table below outlines the supported compatibility.

| Platforms              | Non-CUPS      |         | UPN           |         |
|------------------------|---------------|---------|---------------|---------|
|                        | Non - Overlap | Overlap | Non - Overlap | Overlap |
| GigaVUE-HC3 Gen 3      | ✓             | ✓       | ✓             | ✓       |
| GigaVUE-HC1-Plus Front | ✓             | ✓       | ✗             | ✗       |
| GigaVUE-HC1-Plus Rear  | ✓             | ✓       | ✗             | ✗       |

## Configuring Rotational Sampling in GigaVUE-FM

GigaVUE-FM allows you to configure Rotational Sampling in the second level map of GTP Flow Sample and GTP Flow Overlap.

**NOTE:** The same configuration applies to UPN, with *3GPP node role* for the GigaSMART group as **user** and **mode** as *standalone*.

To configure Rotational Sampling in second level maps, do the following:

3. On the left navigation pane, click on .
4. Go to **Physical > Nodes > Cluster ID**.
5. Go to **Traffic > Maps**.
6. Click **New**.
7. Enter the Map information:
  - a. Enter an alias for the map.

- b. Enter a description about the map.
- c. Select the Type as **Second level**.
- d. Select the Subtype as any one of the following to configure Rotational Sampling:
  - Flow Sample GTP
  - Flow Sample Overlap
- e. Enable the **Rotational Flow Sampling** check-box.

**NOTE:** In GigaVUE-FM, enabling Rotational flow Sampling means it selects the flow sampling type (fstype) as "rotational." Disabling the check-box means the flow sampling type is "default." The "fstype" is only applicable for 'secondLevel/flowSample' and 'secondLevel/flowSampleOverlap' map types.

- f. Enter the percentage of sessions to be sampled in the given interval in the **Offset** range.
  - g. Enter the **Timer** range in minutes. The value ranges from 15 to 45000 minutes.
8. Refer to [Create a New Map](#) section to complete the configuration for rotational sampling.
9. To enable Dynamic Session sampling , under *Map Configuration and Rules* , select the **Periodic Recalculation** flag.

**NOTE:** In GigaVUE-FM , you can edit only the *Periodic Recalculation* flag in existing map rules.

← Back to Node

New Map

OK Cancel

Overview

Health

Save Co...

SYSTEM

Chassis

> Ports

> GigaSMART

> Inline Bypass

TRAFFIC

Maps

Map ...

Filter ...

Map Info

Map Alias \* Profile1 ?

Description

Enable ☒

Type Second Level

Subtype \* Flow Sample GTP

Rotational Flow Sampling ☒ ?

Offset (%) \* 22

Timer (mins) \* 22

Map Source and Destination

Port Editor

Source \* Select ports...

Destination \* Select ports...

Encapsulation Tunnel None

GigaSMART Operations (GSOP) \* FmAuto-gsop-SSL\_App1-6f8896d5-ead... x

Tool Finder

Map Configuration & Rules

Add a Rule ?

Rule 1

Condition

GTP

Periodic Recalculation ☒ ?

Priority 1

Percentage 22

IMEI IMEI

IMSI IMSI

You can also configure Rotational Sampling through Ansible. Refer to [Installation and Configuration of Subscriber Intelligence Solution using Ansible](#) to know more.

You can also configure rotational sampling through GigaVUE-OS CLI. Refer to the `map` and `show map fs-stats all` commands in the GigaVUE-OS CLI Reference Guide to know more.

## Viewing the Configuration of Rotational Sampling for non-CUPS LTE and UPN

After configuring rotational sampling, GigaVUE-FM allows you to view the configuration for non-CUPS LTE and UPN. To view the configuration in GigaVUE-FM, follow these steps:

1. From the left navigation pane, go to **Inventory > Physical > Nodes**.
2. In the **Map Statistics** page you can view the column **Rotational Sampling** which can be either **Enabled** or **Disabled**. If the **Rotational Sampling** is **Enabled**, it would provide a quick link view.

rot-samp > Maps

Maps

Map Groups

Statistics

🔍

🔄

🔔

👤

🏠

📶

📄

← Back to Nodes

Overview

Health

Save Config...

SYSTEM

Chassis

> Ports

> GigaSMART

> Inline Bypass

TRAFFIC

> Maps

Maps

Map Te...

Filter Te...

SETTINGS

> Settings

> Roles and ...

SUPPORT

Logs

> Debug

About

Refresh

Troubleshoot

Filter

Clear

Export

| <input type="checkbox"/> | Map Alias            | Total Counters |          |         |         |        |             |             |             |            |         |            | Rules | Rotation... <sup>+</sup> |
|--------------------------|----------------------|----------------|----------|---------|---------|--------|-------------|-------------|-------------|------------|---------|------------|-------|--------------------------|
|                          |                      | Accepted       | Rejected | Matched | Packets | Octets | Rejected... | Rejected... | Matched ... | Matched... | Entries | IP CAN ... |       |                          |
| <input type="checkbox"/> | FmAuto-gtp1_pod2...  | 0              | 0        | 0       | 0       | 0      | 0           | 0           | 0           | 0          | 0       | 0          | 1     | <a href="#">Enabled</a>  |
| <input type="checkbox"/> | rotationalsampleena  | 0              | 0        | 0       | 0       | 0      | 0           | 0           | 0           | 0          | 0       | 0          | -     | Disabled                 |
| <input type="checkbox"/> | FmAuto-test1-7f2e... | 0              | 0        | 0       | 0       | 0      | 0           | 0           | 0           | 0          | 0       | 0          | 1     | Disabled                 |
| <input type="checkbox"/> | FmAuto-test1-0ae5... | 0              | 0        | 0       | 0       | 0      | 0           | 0           | 0           | 0          | 0       | 0          | -     | Disabled                 |
| <input type="checkbox"/> | FmAuto-sampleMap...  | 0              | 0        | 0       | 0       | 0      | 0           | 0           | 0           | 0          | 0       | 0          | -     | Enabled                  |

⏪

Go to page: 1 of 1

⏩

Total Records: 5

FM Instance: GigaVUE-FM

Node Sync Time: Jul 22, 2022 16:57:06

Last Updated At: Jul 22, 2022 16:54:06

The quick view contains the following columns:

- Current Offset Amount
- Remaining Sampling Time
- Current Interval Start
- Next Interval Start

| Map Alias                                     | Accepted | Rejected | Matched | Packets | QoS |
|-----------------------------------------------|----------|----------|---------|---------|-----|
| <input type="checkbox"/> FmAuto-gtp1_pod2...  | 0        | 0        | 0       | 0       | 0   |
| <input type="checkbox"/> rotationalsampleena  | 0        | 0        | 0       | 0       | 0   |
| <input type="checkbox"/> FmAuto-test1-7f2e... | 0        | 0        | 0       | 0       | 0   |
| <input type="checkbox"/> FmAuto-test1-0ae5... | 0        | 0        | 0       | 0       | 0   |
| <input type="checkbox"/> FmAuto-sampleMap...  | 0        | 0        | 0       | 0       | 0   |

| Map Alias : FmAuto-test1-7f2e2415-cf09-4b0e-ae57-5e2f44a33baa                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div> <div>Current Offset Amount</div> <div>Remaining Sampling Time</div> <div>Current Interval Start</div> <div>Next Interval Start</div> </div> <div> <div>8600</div> <div>4 mins</div> <div>2022-07-22 17:02:10</div> <div>2022-07-22 17:02:10</div> </div> |
| Total Items : 1                                                                                                                                                                                                                                                |

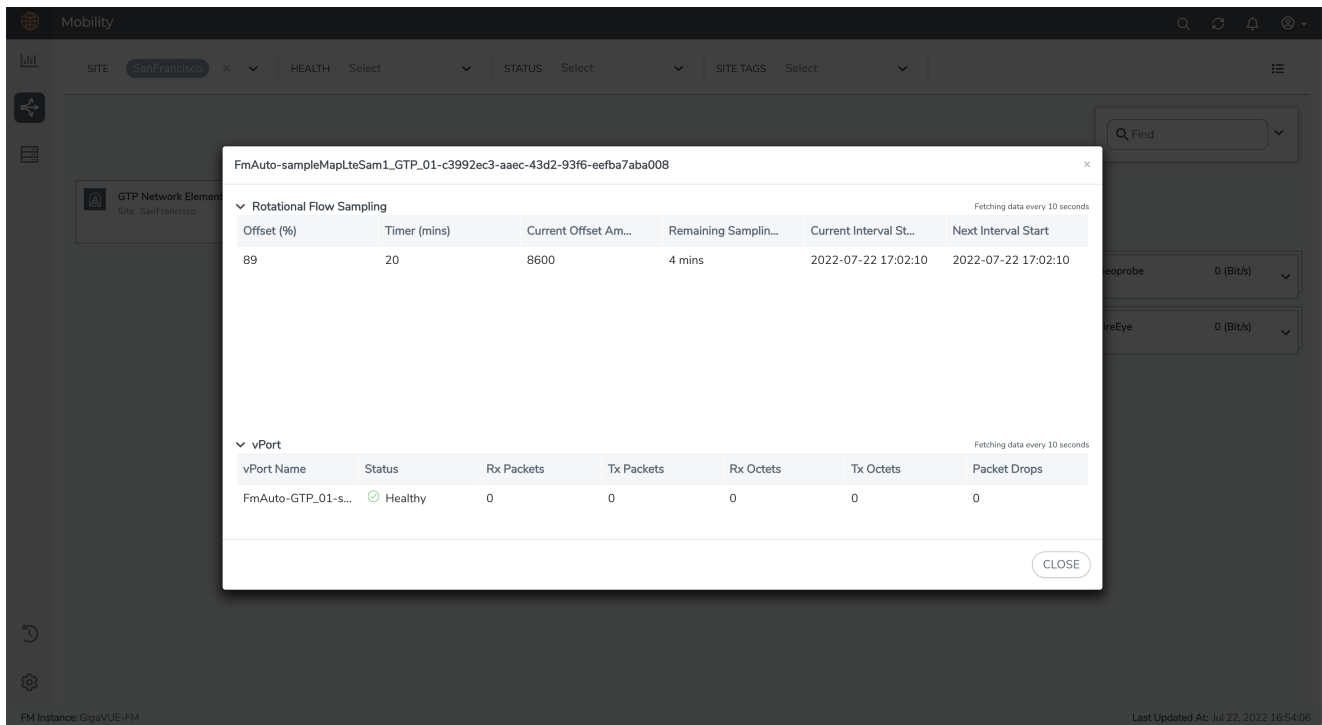
The Rotational Flow Sampling is also supported in the legacy maps pages in GigaVUE-FM. You can create and edit the "fstype" properties from the legacy Maps pages in GigaVUE-FM GUI.

### View a Rotational Sampling configuration in Mobility Solution

If you have configured Rotational Sampling through Ansible, then to view the configuration in GigaVUE-FM, do the following:

1. On the left navigation pane, click on  select **Physical > Orchestrated Flows > Mobility**, and then select the required cluster or node ID.
2. Select the required site from the **Site** drop-down list box.
3. From the **Rules to Destination Tools** block, select the drop-down, and click on the ellipses named as **Details**.
4. A Details-Rules to Geoprobe page appear. In the left-navigation page, click on the **Second Level Maps**.
5. Click on the **Show Details** for the required **Fabric Map Name**.
6. A page with details of Flow Sampling appears. In this page, you can view the details of rotational sampling such as **Offset**, **Timer**, **CurrentOffset Amount**, **RemainingSampling**.

**NOTE:** When configuring rotational sampling in UPN, the *3GPP node role* for the GigaSMART group is **user** and **mode** is *standalone*.



## GigaSMART 4G RAN Correlation

### Required License:

A Radio Access Network (RAN) is part of a telecommunications system that connects individual radio devices to the core mobile network through radio connections.

RAN uses GTP correlation. It exposes RAN data fields from control plane (S11), for example:

- E-UTRAN Cell Global Identifier (ECGI)
- Tracking Area Identity (TAI)
- Tracking Area Code (TAC)

The above identifiers are extracted from the User location Information (ULI) and sends them to flow sampling and whitelisting.

The RAN correlation for 4G CUPS flow sampling filters require the ECGI, TAC and PLMN-ID values.

For 4G RAN based whitelisting requires ECGI includes the PLMN Id and the E-UTRAN Cell ID.

RAN data fields are available for filtering. GigaVUE-FM enables you to configure RAN based correlation for both 4G CUPS and 5G CUPS in the Flow Sample and Whitelist Maps. In CUPS solution, you can configure the RAN Correlation properties while creating and editing the properties in Flow Sample and Whitelist maps in Global policies for both CPN and UPN.

## Rules and Notes

Keep in mind the following rules and notes when you work with the RAN Correlation feature:

- RAN correlation is not supported for the 3G.
- You must configure separate flow sampling map for 3G sampling parameters and 4G RAN sampling parameters to support 3G correlation and 4G RAN correlation in the same GSgroup.

## GigaSMART SIP/RTP Correlation

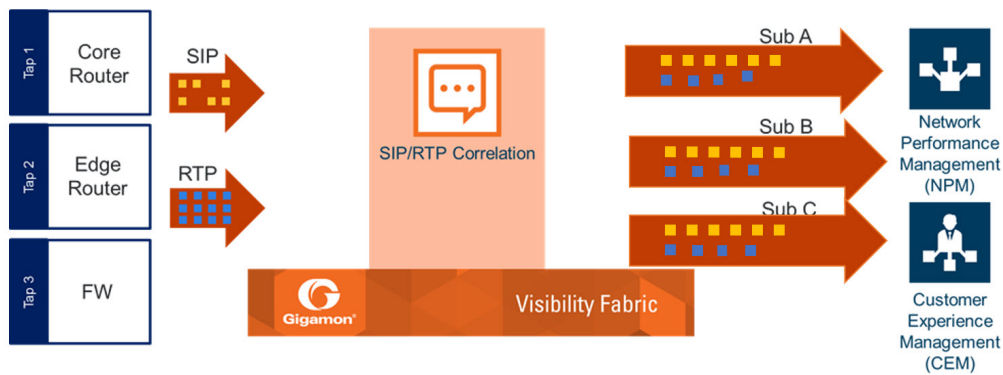
Required Licenses: SIP/RTP Correlation (and FlowVUE for session-aware load balancing for RTP)

Supported Devices : GigaVUE-HC3 Gen 2 and GigaVUE-HC1 Plus.

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

Session Initiation Protocol (SIP) is the dominant method to initiate, maintain, modify, and terminate voice calls in service provider and enterprise networks. Real-time Transport Protocol (RTP) is used to manage the real-time transmission of voice payload across the same networks. Visibility into a subscriber's voice traffic requires the ability to understand the subscriber attributes and stateful information contained within SIP to correlate subscriber-specific RTP traffic so that monitoring tools can achieve an accurate view of the subscriber's traffic on the network.

The GigaSMART SIP/RTP correlation application correlates the subscriber-specific attributes and the endpoint identifiers of the RTP streams where the session is carried, as well as other SIP-related attributes that are exchanged as part of the control sessions. Use SIP/RTP correlation to leverage a subscriber-aware monitoring policy on Gigamon's Deep Observability Pipeline and to optimize current tool infrastructure investments by providing only relevant data to tools while increasing visibility into subscriber traffic. This helps improve QoE and performance. Carriers gain access to the subscriber's traffic by reliably correlating and passing all the identified subscriber's control and data sessions to the analytics/monitoring probes and/or billing subsystems for an accurate view of the subscriber's sessions.



**Figure 5** SIP/RTP Correlation

SIP is a signaling protocol for VoIP and VoLTE call initiation. It is implemented with RTP to control the payload. GigaSMART SIP/RTP correlation provides customers visibility into VoIP, VoLTE, SMSoLTE, and RCS traffic, and allows them to filter and forward traffic for a subscriber to the tools.

All SIP traffic is sent to all tool ports, as follows:

- all SIP packets sent to all ports within a load balancing port group.
- all SIP packets sent to all ports within a GigaStream.
- all SIP packets sent to all tool ports belonging to maps.

RTP traffic will be sampled and sent to the maps with the rules that match. RTP non-correlated traffic will be sent to the collector.

SIP/RTP correlation can be used for both enterprise and service providers, where ever there is SIP/RTP traffic, such as in wire-line communications, wireless communications, and packet cable networks. This includes enterprise, IP Multimedia Subsystem (IMS), or fixed network implementations of SIP, as well as any media controlled by SIP, such as voice, text, or streaming media.

In addition, SIP/RTP correlation correlates SIP signaling and RTP payload for all sessions selected by a SIP User Agent (UA), a caller ID in a forward list, with flow sampling from 0 to 100%.

#### CallerID Tracking

The CallerID is tied to the Call-ID and remains constant for the duration of the session:

**CallerID (A) <-----<Call-ID>-----> CalleeID (B)**

CallerID tracking is based on the initial caller (A) and does not change until the Call-ID changes. Even if the callee, (B), sends a new INVITE during the SIP session, if that INVITE uses the same Call-ID, then the CallerID information in the SIP session display will still identify the initial caller, (A); it will not switch to reflect that (B) is now the caller.

#### Support for SIP, RTP, and RTCP

SIP/RTP correlation handles all SIP signaling and RTP/RTCP traffic, including RTCP control traffic, as well as that belonging to a call session.

The following is supported:

- Non-tunneled SIP, RTP, and RTCP correlation (all IMS interfaces)
- Tunneled SIP, RTP, and RTCP correlation (SIP/RTP/RTCP in GTP-U, through the GTP tunnel)

#### SIP/RTP Correlation Engine

When a packet containing SIP, RTP, or RTCP traffic is received, the SIP/RTP correlation engine looks up the session in the session table for load balancing ports and sampling maps or whitelist map. All SIP/RTP traffic with port or load balancing port group is forwarded based on the session table. The correlation engine load balancing keeps track of both the SIP session and the associated multiple RTP channels.

Each session identifies both sides of media streams (RTP) associated with the session. The SIP session has an aging timer that is configurable.

When a session matches one of the configured flow sampling rules, it is either accepted for sampling or rejected. If it is accepted, all packets belonging to that session are sent to the tool port. Otherwise, all packets belonging to the session are dropped.

#### Configure SIP/RTP Correlation Engine

To configure SIP/RTP Load balancing, follow these steps:

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Group** and then click **New**.
2. Specify an Alias in the **Alias** field.
3. Select Load Balance in **TCP Application Parameters**.
4. Specify the parameters. The following table explains the parameters for configuring the load balance:

| TCP Application Parameters | Options                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application                | <ul style="list-style-type: none"> <li>Broadcast - All the TCP handshake packets are broadcasted to the tool ports in all the maps.</li> <li>Drop - All the unknown application packets of 5G are sent to the collector.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Load Balance               | <ul style="list-style-type: none"> <li>Enable - Select Enable to perform any of the following: <ul style="list-style-type: none"> <li>SIP and RTP packets matching the flowsampling or whitelist maps are loadbalanced across the tool ports within a port-group. The SIP and RTP packets are loadbalanced to the same tool ports.</li> <li>SIP and RTP packets matching the flowsampling or whitelist maps are sent to the tool port.</li> <li>SIP and RTP packets matching the flowsampling or whitelist maps are sent to a tool GigaStream. The SIP and RTP packets may not be loadbalanced to the same tool ports within the GigaStream.</li> </ul> </li> <li>Disable - Select disable to perform any of the following: <ul style="list-style-type: none"> <li>all SIP packets sent to all ports within a load balancing port group</li> <li>all SIP packets sent to all ports within a GigaStream</li> <li>all SIP packets sent to all tool ports belonging to maps</li> </ul> </li> </ul> |
| TCP Control                | <ul style="list-style-type: none"> <li>Broadcast - All the tcp handshake packets will be broadcasted to the tool ports in all the maps..</li> <li>Drop - All the TCP handshake packets will be sent to collector if configured</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

RTP traffic will be sampled and sent to the maps with the rules that match. RTP non-correlated traffic will be sent to the collector.

Only one SIP interface type is supported per engine, for example, S5. There is no mixing of interface types, such as S5 GTP-U with SGi.

#### SIP Whitelist

The SIP whitelist contains caller IDs, callee ID, the range for caller IDs, the range for callee IDs and the IP address. Each forward list entry in a file is a SIP caller ID, callee ID, caller ID range, callee ID range or IP address. The forward list can contain all types of entries.

forward list entries can be alphabetic, IP address, and numeric. For each entry, specify up to 64 alphanumeric characters. Some special characters are also supported.

You can manually add one entry at a time to a whitelist file, or you can upload files in.txt format. You must provide the whitelist caller ID range in numeric. You can also provide multiple entries to the forward list by ID range configuration. Each whitelist file can have up to 20,000 entries. One or more whitelist files can be fetched from a local directory or remote URL using HTTP or SCP.

On GigaVUE-HC3 nodes, the forward list database supports 1 million entries.

Multiple forward list databases can reside on a GigaVUE-FM,GigaVUE HC Series node, but only one forward list is applied to a GigaSMART group at a time.

Only one whitelist map is supported for a GigaSMART group. The GigaSMART operation does not have any rules for forward listing.

#### **RTP Flow Sampling**

FlowVUE is used for session-aware (stateful) load balancing and forward listing with sampling. Only RTP traffic will be sampled. There is no sampling of SIP traffic.

Up to five flow sample maps per GigaSMART group are supported. Each flow sample map can have 20 rules. Use rules to filter on caller ID. The rules support both alphabetic and numeric characters, up to 64 characters. Some special characters are also supported, such as wildcard characters.

Sampling is based on caller ID only (the from field).

#### **Support for Sessions**

The number of supported SIP and RTP sessions are as follows:

- GigaVUE-HC3—1 million SIP sessions and 4 million concurrent RTP sessions

Each SIP session can handle two RTP streams in both directions (bidirectional).

The number of supported TCP sessions are as follows:

- GigaVUE-HC3—2 million sessions

#### **Support for IPv4 and IPv6**

SIP is a text-based protocol, which is supported over UDP and TCP. The size of the

SIP message can vary greatly, so fragmentation and segmentation are common and are supported for tunneled SIP and non-tunneled SIP (IMS).

IPv4 and IPv6 are supported as follows:

- UDP Fragmentation—in-order packets, out-of-order packets
- TCP Segmentation—in-order packets, out-of-order packets

The following is not supported:

- GTP tunneled packets where the inner IP is fragmented
- IMS packets where the outer IP is fragmented

|     |      | UDP        |            |          |              | TCP          |          |              |
|-----|------|------------|------------|----------|--------------|--------------|----------|--------------|
|     |      | Outer Frag | Inner Frag | In order | Out of order | Segmentation | In order | Out of order |
| GTP | IPv4 | ✓          | x          | ✓        | ✓            | ✓            | ✓        | ✓            |
|     |      | ✓          | x          | ✓        | ✓            | ✓            | ✓        | ✓            |
|     | IPv6 | ✓          | x          | ✓        | ✓            | ✓            | ✓        | ✓            |
|     |      | ✓          | x          | ✓        | ✓            | ✓            | ✓        | ✓            |
| IMS | IPv4 | N/A        | ✓          | ✓        | ✓            | ✓            | ✓        | ✓            |
|     |      | N/A        | ✓          | ✓        | ✓            | ✓            | ✓        | ✓            |
|     | IPv6 | N/A        | ✓          | ✓        | ✓            | ✓            | ✓        | ✓            |
|     |      | N/A        | ✓          | ✓        | ✓            | ✓            | ✓        | ✓            |

**Figure 6** SIP/RTP UDP/TCP Support

#### Support for Content Masking

SIP Common Presence and Instant Messaging (CPIM) content masking is supported, but only when the SIP transport is UDP.

The SIP method, MESSAGE, carried over UDP, might contain user-friendly, readable text messages. Use masking to replace these messages with x's, so they cannot be read.

**NOTE:** SIP/RTP correlation cannot mask text messages with a content type other than message/CPIM, such as plain text.

#### Behaviors of Some SIP Methods

The following are behaviors for some particular SIP methods:

- The SIP method, REGISTER, might not contain a user part. When there is no user part, it will be treated as a parse error.
- The SIP method, OPTIONS, (and response messages) might not contain a user part. When there is no user part, it will be treated as a parse error.

**NOTE:** SIP TCP packets with parse errors are not sent to collector. SIP TCP packets will be sent to the tool and incremented as parse errors in the session table stats.

#### SIP Whitelisting in a Cluster

The forward list (all whitelist files) reside on the leader of the cluster. The member nodes receive a copy of the forward list from the leader. Updates to the forward list are synchronized from the leader to the non-leaders. If a member node leaves the cluster and rejoins, its forward list will be resynchronized.

Use the cluster leader preference command to specify the highest preference for the leader, the second highest preference for the standby node, and lower preferences for the normal nodes in the cluster.

If there are GigaVUE TA Series nodes in the cluster, they will not receive a copy of the forward list.

#### Support for NAT

GigaSMART SIP Correlation engine correlates NAT/PAT enabled SIP/RTP packets. The correlation engine compares the top most "Via" address and the contact address of the device with the Layer 3 network address to find whether the device is configured with NAT.

To enable the NAT support, from the device view:

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Groups > SIP > SIP NAT**.
2. Enable the **SIP NAT** check box.

#### Not Supported by SIP/RTP Correlation

The following list is not currently supported by SIP/RTP correlation:

- encryption
- filtering based on Codecs
- SRVCC
- roaming
- SIP-I/SIP-T (supports SIP/RTP correlation based on SDP processing even if SIP carries SIP-I/SIP-T messages)
- forwarding of emergency calls to specific tools
- engine grouping. Only one engine is used for SIP/RTP correlation.

**NOTE:** SIP/RTP correlation and GTP correlation are not supported on the same GigaSMART engine port.

#### Display SIP/RTP Reports

To display SIP report, do the following:

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Groups> Report**.
2. Select Group Type: **Flow SIP**.
3. From the device view, select GigaSMART Group: **gsg1**
4. Specify **Caller ID Pattern**.
5. Select Any. This return any pattern specified in the Caller ID Pattern field.

GigaSMART Groups

GigaSMART Groups

Statistics

Report

Generate

▼ Report Info

Type

Flow SIP

GigaSMART Groups

Select...

Caller ID Pattern

Type Caller ID pattern...(e.g. 5551231234 or 555\*)

☒ Any

Figure 7 Generate SIP Report

6. Click the Generate button. The SIP Messages Report displays.

Caller ID Pattern: Type Caller ID pattern...(e.g. 5551231234 or 555\*) ☒ Any

▼ Sessions Summary

▼ SIP Messages

Total: 15

| SIP     | Tool Pass | No Session | No Rule | No Match | Drop | Other |
|---------|-----------|------------|---------|----------|------|-------|
| ACK     | 0         | 0          | 0       | 0        | 0    | 0     |
| BYE     | 0         | 0          | 0       | 0        | 0    | 0     |
| CANCEL  | 0         | 0          | 0       | 0        | 0    | 0     |
| INFO    | 0         | 0          | 0       | 0        | 0    | 0     |
| INVITE  | 0         | 0          | 0       | 0        | 0    | 0     |
| MESSAGE | 0         | 0          | 0       | 0        | 0    | 0     |
| NOTIFY  | 0         | 0          | 0       | 0        | 0    | 0     |
| OPTIONS | 0         | 0          | 0       | 0        | 0    | 0     |
| PRACK   | 0         | 0          | 0       | 0        | 0    | 0     |

Figure 8 SIP Report Page

Display SIP Map Statistics

Map Statistics displays the counts sessions that matched a particular map.

For SIP Flow Sample maps, the counters show how many sessions matched the Caller-ID rule and were either accepted or rejected based on the sampling percentage.

For SIP Whitelist maps, the counter shows how many total entries are in the Whitelist and how many sessions matched those entries. .

To display SIP Map Statistics, do the following:

- On the left navigation pane, go to **Inventory** from **Traffic** select **Maps> Statistics**. The Statistics page displays a count of the rules that actually matched in a map.

| Map Alias   | Total Counters                    | Rules |
|-------------|-----------------------------------|-------|
| map-sip-1   | 0 Packets, 0 Bytes                | 2     |
| map-sip-551 | 0 Accepted, 0 Rejected, 0 Matched | 2     |
| map-sip-391 | 0 Matched, 2 Entries              | 1     |

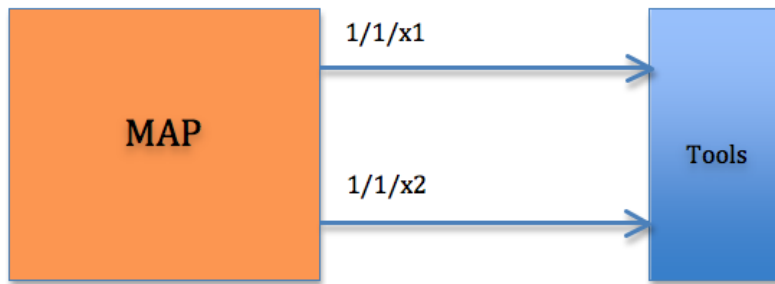
Total Items : 3

Figure 9 SIP Map Statistics

### SIP/RTP Support for Tool Throttling

GigaSMART supports sampling/scaling based on fixed percentages, which remain in effect at all times, regardless of the tool port utilization. However, tool utilization may not be as efficient as not using fixed percentage for every use case. Starting with GigaSMART version 5.4 support for throttling sessions based on the traffic (pps) reaching a tool port is available. This feature helps avoid packets being drops during peak times by allowing users to adjust throttling start and stop levels.

The illustration below is a configuration and Intra Flow for Tool Port Throttling.



### Admission Control

Each SIP session comes with RTP streams and each of the RTP stream uses a specific codec for information transfer. We can use this codec information to our advantage and do predictive analysis on how much pps would be generated for a given SIP session.

Based on the outcome of the pps for a given RTP stream codec, admission control module will check this value against the cumulative packet throughput on the destination tool-port to decide if the session will be Accepted or Rejected.

Example: Tool port 1/1/x1 is configured with a threshold of 3k pps.

| Time | Port   | Session | Codec (pps) | Cumulative pps | Throttle pps | Accepted |
|------|--------|---------|-------------|----------------|--------------|----------|
| t0   | 1/1/x1 | 0       |             | 0              | 3000         |          |
| t1   | 1/1/x1 | 1       | 500         | 500            | 3000         | Yes      |
| t2   | 1/1/x1 | 2       | 1500        | 2000           | 3000         | Yes      |

| Time | Port   | Session | Codec (pps) | Cumulative pps | Throttle pps | Accepted |
|------|--------|---------|-------------|----------------|--------------|----------|
| t3   | 1/1/x1 | 3       | 800         | 2800           | 3000         | Yes      |
| t4   | 1/1/x1 | 4       | 500         | 3300           | 3000         | No       |

In software version 5.4 Tool port throttling applies only to SIP sessions for audio and only load balanced ports are supported in tool port throttling. Use case where there are tapping multiple interfaces using multiple engines, one SIP session can be throttled in one engine and not in another.

## SIP/RTP Examples

This section provides information about:

- [SIP/RTP Load Balancing Example](#)
- [SIP/RTP Minimum Configuration Example](#)

## SIP/RTP Load Balancing Example

This is a load balancing configuration example of SIP/RTP.

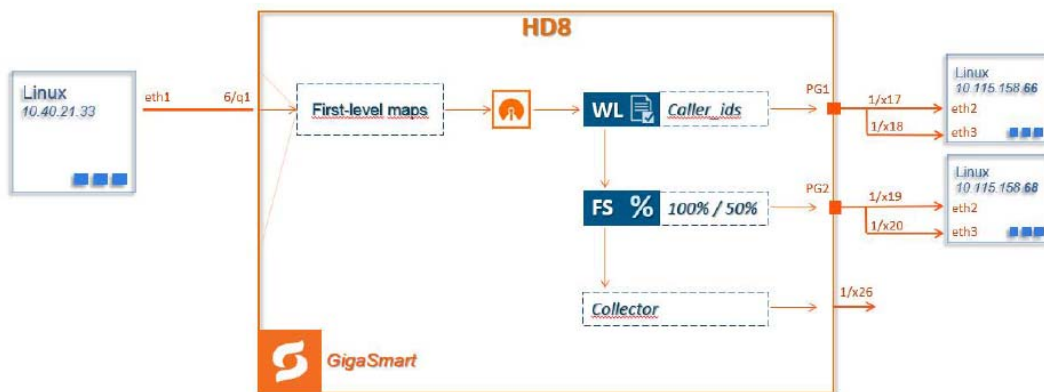


Figure 10 SIP/RTP UDP/TCP Support

## SIP/RTP Minimum Configuration 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.

## Configure ports

To configure a GigaSMART group and associate it with a GigaSMART engine port do the following.

1. 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. **GigaSMART Groups**.
2. Click **New**.
3. Type an alias in the Alias field and enter **an engine port** in the Port List field.

GigaSMART Group OK Cancel

▼ GigaSMART Group Info

Alias

Port List Select ports...

▼ GigaSMART Parameters

› Cross Packet Match

› Resource Buffer

› Metadata Exporter

› Dedup

› Engine Timer

› Generic Session Timeout

› Flow Sampling

› Flow Mask

› Inline SSL

▼ Passive SSL

|                                   |                                                                               |
|-----------------------------------|-------------------------------------------------------------------------------|
| Enable                            | <input checked="" type="checkbox"/>                                           |
| Keymap                            | <span>Visit SSL Services</span>                                               |
| Session Timeout (seconds)         | <input type="text" value="300"/>                                              |
| Pending Session Timeout (seconds) | <input type="text" value="60"/>                                               |
| TCP SYN Timeout (seconds)         | <input type="text" value="20"/>                                               |
| Decrypt Fail Action               | <input checked="" type="radio"/> Drop <input type="radio"/> Pass to Tool Port |
| Key Cache Timeout (seconds)       | <input type="text" value="10800"/>                                            |
| Ticket Cache Timeout (seconds)    | <input type="text" value="10800"/>                                            |

Non SSL Traffic ☒ Drop ☐ Pass to Tool Port

HSM Group Select HSM Group

▼ Load Balance

Failover Enable ☐

Least Bandwidth Failover Threshold (%)

**Figure 11** *GigaSMART Group Port Info*

4. Click **Save**.
5. Scroll down the page to select **SIP Port** parameters.
6. Type parameters for **SIP Port** and **RTP Port**.
7. Enter parameters for **SIP Session Timeout** and the **SIP TCP Idle Timeout**.

The screenshot shows the 'GigaSMART Group' configuration interface. It includes sections for GTP Persistence File Age Timeout (30 minutes), GTP Backup Files (with a 'Delete All' button), GTP Whitelist (with a 'GTP Whitelist Alias' dropdown set to 'None'), and SIP parameters. The SIP section includes 'SIP Flow' with 'Session Timeout (seconds)' (30), 'Media Timeout (seconds)' (30), and 'SIP TCP Idle Timeout (seconds)' (20). It also has a 'SIP Whitelist' section with an 'Alias' dropdown set to 'None'. The 'SIP Ports' section shows 'SIP Port' (5060, 5061) and 'RTP Port (seconds)' with a range from 'Min' (1) to 'Max' (6500).

**Figure 12** *SIP Port parameters*

8. Click **OK**.

## Create Virtual 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.

To create virtual ports, do the following:

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

The screenshot shows the 'Virtual Ports' configuration dialog. It includes fields for 'Alias' (vport1), 'GigaSMART Group' (a dropdown), 'Mode' (GTP Overlap), 'Inline Failover Action' (Virtual port bypass), and 'ASF Profile' (Select ASF Profile...). There are 'OK' and 'Cancel' buttons at the top right. A note states: 'Note: Default fail over action for vport is Virtual port bypass.'

**Figure 13** *Virtual Ports*

3. Enter an **alias** in the Alias field to identify the virtual port.
4. In the GigaSMART Groups field, select the GigaSMART Group configured in Step 1: of Configure a GigaSMART Group.
5. Click **Save**.

## Configure GigaSMART Operation

Define a GigaSMART operation to enable SIP Flow Sampling. If combining Flow Sampling with Load Balancing GSOPs, make sure that you select both operations when creating the GigaSMART Operation.

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 GigaSMART Operation, do the following:

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Operations (GSOP)**.
2. Click **New**. On the GigaSMART Operations page, do the following:

GigaSMART Operation (GSOP) [OK] [Cancel]

Alias: gsop\_sip\_FS\_lb

GigaSMART Group: gsg1

GigaSMART Operations (GSOP): [dropdown arrow]

**Flow Sampling** [x]

Flow Sampling - GTP ☐

Flow Sampling - IP ☐

Flow Sampling - SIP ☒

**Figure 14** *GigaSMART Operations page*

3. In the Alias field, enter an **alias** to help identify this GSOP.
4. In the **GigaSMART Groups field**, select the **GigaSMARTgroup** configured in Step 1: Configure a GigaSMART Group.
5. In the GigaSMART Operations (GSOP) field, select **Flow Samplingfor SIP**.
6. Using the GSOP drop down list, select **Load Balancing** as the next GSOP operation.

**Figure 15** GigaSMART Operations - Load Balancing

Options:

- Stateful
- Stateless
- Enhanced

7. Select **Stateful**.
8. For Type, select **SIP** as the stateful application within a group of GigaSMART operations.
9. Select **Caller ID** as the Load Balancing Method.
10. Click **OK**.

Create first level map

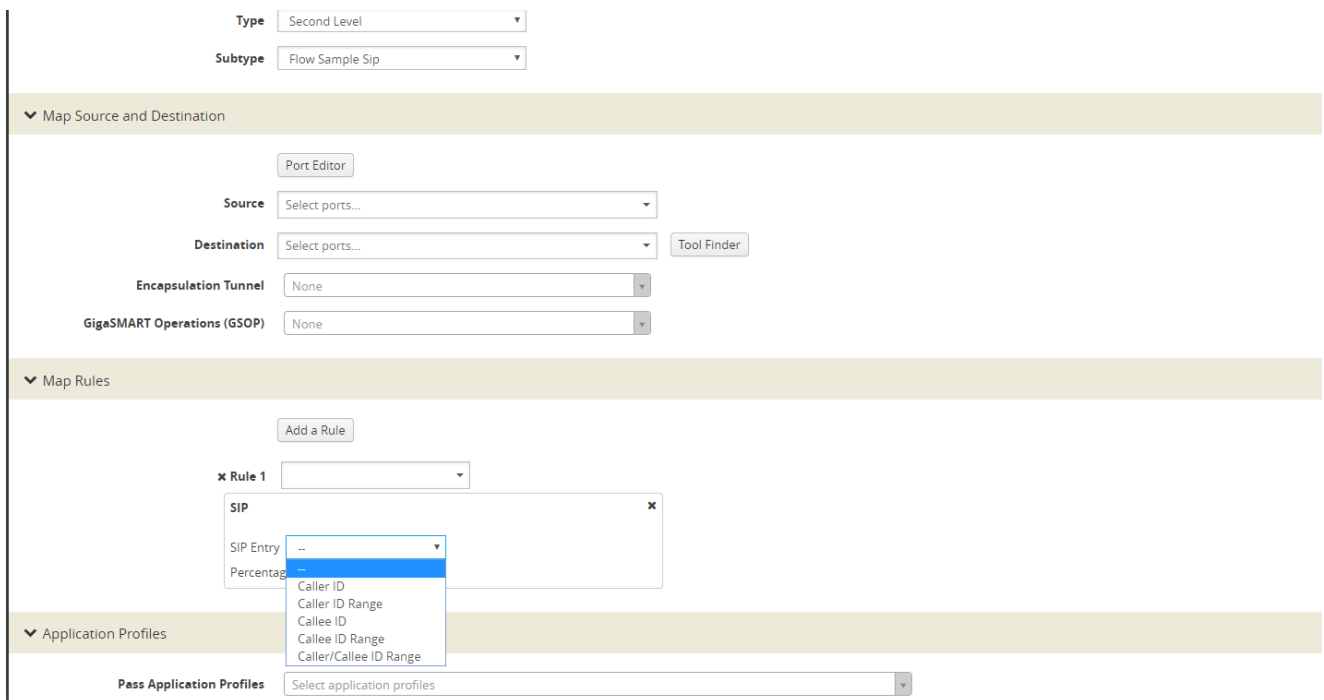
1. On the left navigation pane, go to **Inventory**  from **Traffic** select **Maps > Maps > Maps**.
2. Click **New**.
3. Type **map-level1** in the Alias field.
4. Select **First Level** for Type and **By Rule** for Subtype.
5. Select **port 1/1/x1** for the Source.

**Figure 16** Create New Map

6. Select **virtual port vport1** for the Destination.
7. Click **Adda Rule** to add Rule 1
8. Click **Save**.

### Create second level map for SIP Flow Sampling.

1. On the left navigation pane, go to **Inventory**  from **Traffic** select **Maps > Maps > Maps**.
2. Click **New**.
3. Type **an alias** in the Alias field.
4. Select **Second Level** for Type and **Flow Sample SIP** for Subtype.
5. Select virtual port **vport1** for the Source.
6. Select **port group** for the Destination.
7. Select **the group** from the GSOP list.
8. Click **Add a Rule**.
9. Select **SIP** for the condition.
10. Select any of the following options:
  - o Caller ID-For example, enter **408\*** for Caller ID.
  - o Caller ID Range
  - o Callee ID
  - o Callee ID Range
  - o Caller/Callee ID Range



The screenshot displays the configuration interface for creating a second-level map for SIP flow sampling. The interface is divided into several sections:

- Type:** Set to "Second Level".
- Subtype:** Set to "Flow Sample Sip".
- Map Source and Destination:**
  - Source:** "Select ports..."
  - Destination:** "Select ports..." with a "Tool Finder" button.
  - Encapsulation Tunnel:** Set to "None".
  - GigaSMART Operations (GSOP):** Set to "None".
- Map Rules:**
  - Add a Rule:** Button to add a new rule.
  - Rule 1:** A dropdown menu showing "SIP".
  - SIP Entry:** A dropdown menu showing "--".
  - Percentage:** A dropdown menu showing "--".
  - Condition List:** A list of options for the SIP condition:
    - Caller ID
    - Caller ID Range
    - Callee ID
    - Callee ID Range
    - Caller/Callee ID Range
- Application Profiles:**
  - Pass Application Profiles:** A dropdown menu showing "Select application profiles".

**Figure 17** *Create Second Level Map*

11. Enter a **percentage** for amount the traffic you want to be affected by SIP flow sampling.
12. Click **Add a Rule**.
13. Select **SIP** for the condition
14. Enter **6501234\*** for Caller ID.
15. Enter a **percentage** for amount the traffic you want to be affected by SIP flow sampling.
16. Click **OK**.

### Create the SIP whitelist

1. From the left navigation pane, go to **System > GigaSMART > Whitelist**.
2. Click **New**.
3. Type an **alias** in the Alias field.
4. From the GigaSMART Groups drop-down list, select a .the GigaSMART group.
5. Load whitelist files from a specified location to populate the SIP whitelist.
  - a. On the SIP Whitelist page, select **Bulk Upload**.
  - b. Select **Bulk Entry Operation** for **Upload Type**
  - c. Select Upload from URL from the Bulk Upload Type list.
  - d. Enter the **URL** in the **Enter Remote URL** field.
6. Click **OK**.

### Associate the GigaSMART group to the SIP whitelist.

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Groups > GigaSMART Groups**.
2. Select the **GigaSMART Group** you previously created and click **Edit**.
3. From the **GigaSMART Groups drop-down list**, select a GigaSMART group previously created.
4. Under **SIP Whitelist**, click on the **SIP Whitelist Alias field** and select the **alias** previously created from the available list.
5. Click **OK**.

### Configure GigaSMART operation for SIP whitelisting

1. From the left navigation pane, go to **System > GigaSMART >GigaSMART Operations > GigaSMART Operation**.
2. Click **New**.
3. Type an **alias** in the Alias field.

4. Select the GigaSMART group created in task 1.
5. From the GigaSMART Operations (GSOP) drop-down list, select the following:
  - o **SIP Whitelist** and select **Enabled**.
  - o **Load Balancing**.
6. For Load Balancing, do the following:
  - a. Choose: **Stateful**
  - b. For Type select: **SIP**
7. Click **OK**.

### Configure first level map

1. On the left navigation pane, go to **Inventory**  from **Traffic** select **Maps > Maps > Maps**.
2. Click **New**.
3. Configure the map:
  - a. Enter an **Alias**
  - b. Type: **First Level**, Sub Type: **By Rule**
  - c. Source: **1/1/g2**
  - d. Destination: **vport**
4. Click **Add a Rule**.
5. Click **Save**.

### Create another second level map for SIP flow whitelist

1. Select **Maps > Maps > Maps**.
2. Click **New**.
3. Configure the map:
  - a. Alias: **alias name**
  - b. Type: **Second Level**, Sub Type: **Flow Whitelist SIP**
  - c. Source: **vport1**
  - d. Destination: **1/2x23**
  - e. Select from the **GSOP** list.
4. Click **Add a Rule**.
5. Select SIP. In SIP type, you can choose any of the following options:
  - o **Caller ID**

- Callee ID
  - Caller/Callee ID
  - Source IP
  - Destination IP
  - Source/Destination IP
  - All
6. Click **OK**.

## GigaSMART IP FlowVUE

Required License: FlowVUE

**Supported Devices :** GigaVUE-HC1 Gen 2, GigaVUE-HC1 Gen 3, GigaVUE-HC3 Gen 2, GigaVUE-HC3 Gen 3, GigaVUE-HC1-Plus.

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

The GigaSMART IP FlowVUE application enables existing tools to connect to the latest high-speed pipes by providing a representative view of traffic for diagnostic coverage. It allows organizations to sample traffic based on outer IP address or inner IP address across GTP tunnels. It intelligently reduces the amount of traffic while maintaining the integrity of the traffic by forwarding all the traffic flows associated with the sampled IP to the monitoring and analytic tools.

This feature can be used for troubleshooting, resolving tool's over-subscription, and ensuring optimal utilization of tool licenses.

GigaSMART IP FlowVUE supports the following:

- flow-aware sampling of IPs to filter and forward all flows sourced from a sampled set of IPs.
- random sampling on IPs and IP ranges, and at configurable sampling rates.
- Sampling GTP traffic based on inner IP header.
- User-configurable timeouts to detect and replace inactive IPs.

FlowVUE operations can be assigned to GigaSMART groups consisting of a single GigaSMART engine. Refer to [Groups of GigaSMART Engine Ports](#) for details.

### Configure FlowVUE

The GigaSMART parameters for configuring FlowVUE are as follows:

| GigaSMART Field          | Definition                                                                                                                                                                                                                                                                                                                                        |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                     | Specifies whether inner or outer IP addresses are used for FlowVUE sampling as follows: <ul style="list-style-type: none"> <li>• Device IP—Specifies a sample subset of traffic based on outer IP address.</li> <li>• Device IP in GTP—Specifies a sample subset of traffic based on inner IP address encapsulated in the GTP tunnels.</li> </ul> |
| IPv4 Ranges /IPv6 Ranges | Specifies the range of IPv4/ IPv6 addresses.<br><b>Note:</b> The maximum IPv4 and IPv6 ranges that are configurable are 64 .                                                                                                                                                                                                                      |
| Rate (%)                 | Specifies the rate for random sampling of the traffic. The values range from 5 to 95%.                                                                                                                                                                                                                                                            |
| Timeout (minutes)        | Specifies after how much time a flow in a sampled IP range is declared idle and is no longer sampled. The values range from 1 to 60 minutes.                                                                                                                                                                                                      |

## FlowVUE Configuration Examples

Refer to the following section for examples:

- [Sample a Subset of IP Traffic](#)
- [Required License: FlowVUE](#)
- [Required License: FlowVUE](#)

## Display FlowVUE Statistics

To display FlowVUE statistics, select **GigaSMART > GigaSMART Operations (GSOP) > Statistics**.

Refer to [FlowVUE Statistics Definitions](#) for descriptions of these statistics as well as to [GigaSMART Operations Statistics Definitions](#).

## FlowVUE\_Examples

This section contains:

- [Sample a subset of IP Traffic](#)
- [Sample a subset of Subscribers' IP traffic encapsulated in GTP.](#)
- [Sample a subset of Subscribers' web traffic encapsulated in GTP](#)

## Sample a subset of IP Traffic

The following example samples on traffic (IP) where 10% of the traffic is forwarded.

| Task | Description                                                                                                 | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                                                           | <ol style="list-style-type: none"> <li>1. Go to <b>System &gt; Ports &gt; Ports &gt; All Ports</b>.</li> <li>2. Click Quick Port Editor.</li> <li>3. Configure one network port and two tool ports. For example, select Network for port 1/1/x3. Select Tool for port 1/1/x4 and port 1/1/x1.</li> <li>4. Select Enable for each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                                                                                                                                                                                                             |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port and configure sampling parameters | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>2. Click New.</li> <li>3. Type gsg1 in the Alias field.</li> <li>4. Click into the Port List field and select an engine port. For example. 1/1/e1.</li> <li>5. Configure the Flow Sampling parameters under GigaSMART Parameters. <ul style="list-style-type: none"> <li>o Select Device IP under Flow Sampling type field.</li> <li>o Enter 1.1.1.0/255.255.255.0 in the IP Ranges field.</li> <li>o Enter 10 for Rate to set the flow sampling rate to 10 percent.</li> <li>o Enter Timeout between 1-60.</li> </ul> </li> <li>6. Click Save.</li> </ol> |

| Task | Description                                                             | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group. | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operations</b>.</li> <li>2. Click New.</li> <li>3. Type gsfvue in the Alias field.</li> <li>4. Select gsg1 from the GigaSMART Groups list.</li> <li>5. Select Flow Sampling from the GigaSMART Operations (GSOP) list.</li> <li>6. Select Flow Sampling - IP</li> <li>7. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                         |
| 4    | Create a Regular map.                                                   | <ol style="list-style-type: none"> <li>1. On the left navigation pane, go to <b>Inventory </b> from <b>Traffic</b> and select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>• Enter to tool in the Alias field.</li> <li>• Select Regular for Type.</li> <li>• Select By Rule for Subtype.</li> <li>• Select the network port for the Source.</li> <li>• Select a tool port for the Destination.</li> <li>• Select gsfvue from the GSOP list.</li> </ul> </li> <li>4. Add a rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select Port Destination.</li> <li>d. Enter the port value.</li> </ol> </li> <li>5. Click Save.</li> </ol> |

## Sample a subset of Subscribers' IP traffic encapsulated in GTP.

The following example illustrates sampling and forwarding the 10% of subscriber's traffic (IP address encapsulated in GTP-U traffic) to the security and monitoring tools.

| Task | Description                                                                                                 | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                                                           | <ol style="list-style-type: none"> <li>1. Go to <b>System &gt; Ports &gt; Ports &gt; All Ports</b>.</li> <li>2. Click Quick Port Editor.</li> <li>3. Configure one network port and two tool ports. For example, select Network for port 1/1/x3. Select Tool for port 1/1/x4 and port 1/1/x1.</li> <li>4. Select Enable for each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                                                                                                                                                                                                                    |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port and configure sampling parameters | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>2. Click New.</li> <li>3. Type gsg1 in the Alias field.</li> <li>4. Click into the Port List field and select an engine port. For example. 1/1/e1.</li> <li>5. Configure the Flow Sampling parameters under GigaSMART Parameters. <ul style="list-style-type: none"> <li>o Select Device IP in GTP under Flow Sampling type field.</li> <li>o Enter 1.1.1.0/255.255.255.0 in the IP Ranges field.</li> <li>o Enter 10 for Rate to set the flow sampling rate to 10 percent.</li> <li>o Enter Timeout between 1-60.</li> </ul> </li> <li>6. Click Save.</li> </ol> |

| Task | Description                                                             | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group. | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operations</b>.</li> <li>2. Click New.</li> <li>3. Type gsfvue in the Alias field.</li> <li>4. Select gsg1 from the GigaSMART Groups list.</li> <li>5. Select Flow Sampling from the GigaSMART Operations (GSOP) list.</li> <li>6. Select Flow Sampling - IP</li> <li>7. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 4    | Create a Regular map.                                                   | <ol style="list-style-type: none"> <li>1. On the left navigation pane, go to <b>Inventory </b> from <b>Traffic</b> and select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>• Enter to tool in the Alias field.</li> <li>• Select Regular for Type.</li> <li>• Select By Rule for Subtype.</li> <li>• Select the network port for the Source.</li> <li>• Select a tool port for the Destination.</li> <li>• Select gsfvue from the GSOP list.</li> </ul> </li> <li>4. Add a rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select Port Destination.</li> <li>d. Enter 2152 as the port value.</li> </ol> <p><b>Note:</b> In the rule, 2152 is GTP-U traffic port value.</p> </li> <li>5. Click Save.</li> </ol> |

## Sample a subset of Subscribers' web traffic encapsulated in GTP

By combining FlowVUE with other GigaSMART APF, the traffic can be further reduced by filtering on specific Layer 4 application ports.

The following example samples on a subset of IP address encapsulated in GTP and forwards only the HTTP traffic related to the sampled set of IPs.

| Task | Description                                                                                  | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure one network and two tool type of ports.                                            | <ol style="list-style-type: none"> <li>1. Go to <b>System &gt; Ports &gt; Ports &gt; All Ports</b>.</li> <li>2. Click Quick Port Editor.</li> <li>3. Configure one network port and two tool ports. For example, select Network for port 1/1/x3. Select Tool for port 1/1/x4 and port 1/1/x1.</li> <li>4. Select Enable for each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol>                                                                                                                                                                                                                                                                                   |
| 2    | Configure a GigaSMART group and associate it with a GigaSMART engine port.                   | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>2. Click New.</li> <li>3. Type gsg1 in the Alias field.</li> <li>4. Click in the Port List field and select an engine port. For example. 1/1/e1.</li> <li>5. Configure the Flow Sampling parameters under GigaSMART Parameters. <ul style="list-style-type: none"> <li>o Select Device IP in GTP.</li> <li>o Enter 1.1.1.0/255.255.255.0 in the IP Ranges field.</li> <li>o Enter 10 for Rate to set the flow sampling rate to 10 percent.</li> <li>o Enter timeout between 1-60.</li> </ul> </li> <li>6. Click Save.</li> </ol> |
| 3    | Configure the GigaSMART operation and assign it to the GigaSMART group. Also, configure APF. | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation</b>.</li> <li>2. Click New.</li> <li>3. Type gsfvue_apf in the Alias field.</li> <li>4. Select gsg1 from the GigaSMART Groups list.</li> <li>5. Select APF from the GigaSMART Operations (GSOP) list</li> <li>6. Enable APF.</li> <li>7. Select Flow Sampling from the GigaSMART Operations (GSOP) list.</li> <li>8. Select Flow Sampling - IP</li> <li>9. Click Save.</li> </ol>                                                                                                                                                |

| Task | Description                                                                                                                                                     | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4    | Configure virtual port and associate it with the GigaSMART group.                                                                                               | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt; Virtual ports</b>.</li> <li>Click New.</li> <li>Enter vp1 in the Alias field.</li> <li>Select gsg1 from the GigaSMART Groups list.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 5    | Create a first level map and direct traffic to the virtual port.                                                                                                | <ol style="list-style-type: none"> <li>On the left navigation pane, go to <b>Inventory</b>  from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>Click New.</li> <li>Configure the map. <ul style="list-style-type: none"> <li>Enter to_vp in the Alias field.</li> <li>Select First Level for Type.</li> <li>Select By Rule for Subtype.</li> <li>Select the network port for the Source.</li> <li>Select the virtual port vp1 for the Destination.</li> </ul> </li> <li>Add a rule. <ol style="list-style-type: none"> <li>Click Add a Rule.</li> <li>Select Pass.</li> <li>Select Port Source.</li> <li>Enter the port value.</li> </ol> <p><b>Note:</b> In the rule, 2152 is GTP-U traffic port value.</p> </li> <li>Click Save.</li> </ol>                                                                                                       |
| 6    | Create a second level map and use the APF GigaSMART operation. APF performs filtering according to the gsrules, sending only matching traffic to the tool port. | <ol style="list-style-type: none"> <li>On the left navigation pane, go to <b>Inventory</b>  from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>Click New.</li> <li>Configure the map. <ul style="list-style-type: none"> <li>Enter map1 in the Alias field.</li> <li>Select Second Level for Type.</li> <li>Select By Rule for Subtype.</li> <li>Select the virtual port vp1 for the Source.</li> <li>Select the a tool port for the Destination.</li> <li>Select gsfvue_apf from the GSOP list.</li> </ul> </li> <li>Add a gsrule 1. <ol style="list-style-type: none"> <li>Click Add a Rule.</li> <li>Select Pass.</li> <li>Select Port Destination.</li> <li>Enter 80 for the port value.</li> <li>Select 2 for Position.</li> </ol> </li> <li>Add a gsrule 2. <ol style="list-style-type: none"> <li>Click Add a Rule.</li> </ol> </li> </ol> |

| Task | Description | UI Steps                                                                                                                                                                                              |
|------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | <ol style="list-style-type: none"> <li>b. Select Pass.</li> <li>c. Select Port Source.</li> <li>d. Enter 80 for the port value.</li> <li>e. Select 2 for Position.</li> <li>6. Click Save.</li> </ol> |

## GigaSMART GTP Whitelisting and GTP Flow Sampling

Required Licenses: GTP Filtering & Correlation and FlowVUE

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

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

Use GTP forward listing and GTP flow sampling to provide subsets of GTP correlated flows to tools. GTP forward listing selects specific subscribers based on IMSI, while GTP flow sampling uses map rules to select subscribers. Starting in software version 4.8, GigaSMART supports GTP overlap mapping, which combines both forward listing and flow sampling maps as part of a map group. Refer to [GTP Overlap Flow Sampling Maps](#)

Starting in software version 4.5, a GigaSMART group (gsgroup) associated with GTP applications can have multiple GigaSMART engine port members (e ports), up to four, forming an engine group. Refer to [GTP Scaling](#).

Refer to the following sections:

- [GTP Whitelisting](#)
- [GTP Flow Sampling](#)
- [GTP Subscriber Aware Random Sampling](#)
- [Display GTP Flow Ops Report Statistics](#)

### GTP Whitelisting

GTP forward listing selects specific subscribers based on IMSI. The forward list contains up to 2,000,000 subscriber IMSIs. For subscribers in the forward list, 100% of their traffic is always sent to a specified tool port.

For example, when a subscriber session comes in, GTP forward listing checks the IMSI of the subscriber. If the incoming IMSI or RAN matches an IMSI or RAN in the forward list, the session is sent to the tool port or load balancing group specified in the forward list map.

Starting in software version 4.7, GTP forward listing is supported in a cluster. Refer to [GTP Whitelisting in a Cluster](#) for more information.

## Create Forward List

Subscriber IMSIs are added to a forward list that can contain up to 2,000,000 subscriber IMSIs. You can create multiple forward list database per GigaSMART group but the maximum number of whitelist entries allowed are 2,000,000 IMSIs per GigaSMART group. You can have a maximum of 20 active forward list database in a GigaSMART group. You can also perform dynamic addition of a forward list database after deploying a solution. You can delete the forward list database, only after removing the GigaSMART group. Refer to [Delete Forward List](#).

For the sequences of steps to create a forward list with the UI, refer to the configuration example for forward listing in [Required Licenses: GTP Filtering & Correlation and FlowVUE](#).

Entries in the forward list can be added one at a time or whitelist files containing multiple IMSIs can be created and downloaded. Entries are added by using the GTP Whitelist page by selecting **GigaSMART > GTP Whitelist**. The GTP Whitelist page shows alias for the currently configured GTP Whitelists, the IMSI count for each Forward list and the GigaSMART Group associated with the GTP Whitelist. The GTP Whitelist is associated with the GigaSMART group by specifying its alias in the **GTP Whitelist Alias** field in GigaSMART Group configuration page and then clicking **New**.

An individual IMSI is added by selecting **Individual Entry Operation** and specifying the IMSI in the **Individual IMSI Entry** field.

The IMSIs in whitelist files must be distinct entries, with one IMSI on each line of a file and a maximum of 500,000 entries in each file. This means that 4 files of 500,000 entries will be needed to populate the forward list to its capacity. Wildcards are not supported in whitelist files.

Whitelist files must have a filename with a .txt suffix. Use the GTP Whitelist page to fetch the entries from a whitelist file at a specified location, using one of the following formats, which are specified in the **Enter Remote URL** field when **Bulk Entry Operation** is selected and the **Bulk Upload Type** is **Upload from URL**:

- http://IPAddress/path/filename.txt
- scp://username:password@IPAddress:/path/filename.txt
- tftp://IPAddress/path/filename.txt

To fetch a whitelist file from a local location, select **File Upload** for **Bulk Upload Type** and use the **Browse** button to select the file.

To update an existing forward list, download the whitelist file, add the forward list entry and then re-upload the file. This will not modify or remove the previous entries added in the file.

When a whitelist file is downloaded, the entries are compared to the forward list on the node. There may be new entries in the file that might already be part of the existing forward list. GigaSMART will add the new, non-duplicate entries to the forward list, without rejecting the entire file.

If the current number of entries in the forward list plus the new entries in the whitelist file is greater than the forward list capacity of 2,000,000 IMSIs, the **Append** operation will fail and the new entry or the entries from the new whitelist file will not be added.

GTP forward listing does not use map rules like GTP flow sampling does. The forward list is associated with a GigaSMART group, GigaSMART operation, and second level maps, called whitelist maps.

For the sequences of steps to create a forward list with the UI, refer to the configuration example for forward listing in [Required Licenses: GTP Filtering & Correlation and FlowVUE](#).

## Configure Whitelist Maps

The whitelist maps are configured per GigaSMART group. Each forward list map, associated with the same vport, uses the same underlying forward list.

Up to ten (10) whitelist maps are supported. Multiple whitelist maps provide a granular selection of tool ports for forward listing. Using multiple maps, traffic can be segregated and sent to multiple destinations. Forward list map rules allow you to select the subset of IMSIs sent to a particular tool.

Each forward list map can contain up to four rules. The rules specify the type of traffic to be forward listed by that map. Within any single map, the rules are evaluated in order. The rules in the first map have a higher priority than the rules in the second, third, and subsequent maps.

The rules will specify either an Evolved Packet Core (EPC) interface type or a GTP version as the attribute to match. An Access Point Name (APN) can also be specified in a rule of a Second Level Flow Whitelist map, either by itself, or preceding the EPC interface type or in combination with the GTP version.

For APN, you must specify a pattern (a name) to match. Use APN to direct the traffic that matches the pattern to a specific tool.

GTP version and EPC interface are mutually exclusive. A mix of versions and interface types across whitelist maps, associated with the same vport, is not supported. For example, you can configure two whitelist maps with one map specifying a rule for version 1 and another map specifying a rule for version 2, OR four whitelist maps with each map specifying a rule for each interface type (Gn, S11, S5, and S10). For more information on interfaces, refer to [Supported Interfaces](#).

An APN pattern is for example, three.co.uk. Wildcard prefixes and suffixes are supported, for example, \*mobile.com or \*ims\*. The pattern can be specified in up to 100 case-insensitive alphanumeric characters and can include the following special characters: period (.), hyphen (-), and wildcard (\*). A standalone wildcard (\*) is not allowed for APN.

You must specify a pattern required for the forward list DataBase (DB) lookup in Type. The following three types of values are supported for the DB lookup:

- imsi/supi – only IMSI or SUPI value used for the DB lookup.
- ran – only RAN value used for the DB lookup.
- all – both RAN and IMSI/SUPI value used for the DB lookup.

By default, SUPI or IMSI is value is used for the DB lookup, if no type is configured.

You can configure a maximum of 10 forward list aliases in a single forward list map. The Database lookup happens only in the configured forward list alias based on the configured DB type.

When there is only DB type is configured and no forward list alias is configured, then the first forward list DB configured in the gparams is used for the DB lookup.

When there is no DB type and no forward list alias are configured, then the lookup happens in all the forward list DB configured in the gparams.

Each new subscriber session will be evaluated by the whitelist maps in the order of priority, which, by default, is the order in which the maps were created.

When a subscriber session comes in, GTP forward listing will check the IMSI of the subscriber. If the IMSI is present in the forward list, the rules in the first forward list map is evaluated to qualify the match further. Otherwise, the packet is evaluated against the rules in the subsequent whitelist maps for a possible match.

For example, with one forward list map having a rule specifying GTP version 1 and another forward list map having a rule specifying GTP version 2, when a subscriber session comes in, GTP forward listing will check the IMSI of the subscriber. if the IMSI is present in the forward list and if there is a match to version 1, the session (100% of subscriber packets) will be forwarded to the tool port, GigaStream, or load balancing group specified in the forward list map. If there is not a match to version 1, the next map is evaluated. If there is a match to version 2 in the next map, the session will be forwarded to the tool port, GigaStream, or load balancing group specified in the second forward list map.

**NOTE:** Both maps can specify the same destination.

Rules can be added to, or deleted from, a forward list map. Use the **Add a Rule** button to add a new forward list rule (a pass rule). Click x to delete a rule. A rule in a forward list map cannot be edited. To edit a rule, first delete it, then recreate it.

The default map configuration in which neither GTP version, EPC interface, or APN is specified in the map, continues to be supported. If the incoming IMSI matches an IMSI in the forward list, the session will be sent to the tool port, GigaStream, or load balancing group specified in the forward list map.

Whitelist maps cannot contain any other rules such as GigaSMART rules (gsrule), flow filtering rules (flowrule), or flow sampling rules (flowsample).

GTP whitelist-based forwarding is performed prior to GTP flow sampling (rule-based flow sampling) and GTP flow filtering.

**NOTE:** For GTP second level maps, a maximum of fifteen maps can be attached to a vport. For example, for the same vport you can have five whitelist maps and ten flow sampling maps, or ten whitelist maps, four flow sampling maps, and one flow filtering map. In addition, you can have a collector map, which is not counted.

For the steps to create a whitelist map with the UI, refer to the configuration example for forward listing in [Required Licenses: GTP Filtering & Correlation and FlowVUE](#).

## Change Priority of Whitelist Maps

Use the **Priority** field in the map to change the priority of whitelist maps.

## Delete Whitelist Maps

When a forward list map is deleted, the priority of the remaining whitelist maps will be re-prioritized. For example, if the first forward list map is deleted, the second forward list map will increase in priority.

For the deleted forward list map, the traffic associated with the rules in the map will be reevaluated and then passed to subsequent maps.

When a forward list map is re-prioritized, the existing sessions will be reevaluated according to the new priority of the map. The traffic associated with the rules in the map will be reevaluated and then passed to subsequent maps.

When the last forward list map is deleted, the traffic associated with the rules in the map will also be reevaluated before being passed to subsequent maps. But the traffic associated with the rules in maps that were not matched, will not be reevaluated because that traffic was already passed to subsequent maps.

## Apply Forward List

When a single forward list entry is added, forward listing is applied for new as well as existing subscribers. When a new whitelist file is fetched, forward listing is applied only for new subscribers.

Forward listed traffic is then sent to the port or load balancing group specified in the whitelist map.

## Delete Entry from Forward List

Entries in the forward list can be deleted one at a time. Each entry is a single IMSI.

When a forward list entry is deleted, the session associated with the forward list entry stays active and traffic is still sent to the whitelist map. The forward list session will not be reevaluated or passed to subsequent maps.

To delete a single entry from the forward list, select **Individual Entry Operation**, set **Remove** as the **Operation Type**, and enter the IMSI in the **Individual IMSI Entry** field.

## Delete Multiple Entries from Forward List

Multiple IMSIs can be deleted from the forward list. Specify the IMSIs to be deleted in a whitelist file, which can contain up to 20,000 IMSIs.

Whitelist files must have a filename with a .txt suffix. To remove multiple entries from the forward list, select **Bulk Entry Operation** and set **Remove** as the **Operation Type**.

## Delete Forward List

The entire forward list can be deleted using one of the following options:

- Delete the forward list by deleting all the IMSI entries. With this option, you do not have to delete the forward list map, GigaSMART operation, or disassociate the GigaSMART group from the forward list. To delete all the IMSI entries, select **Delete All**.
- Destroy the forward list. With this option, you must first delete the forward list map, GigaSMART operation, and disassociate the GigaSMART group from the forward list before deleting the forward list.
- Alternatively, select the forward list and click on edit option then select the '**Clear**' radio button, to remove existing forward list.

## Destroy Forward List

To destroy a forward list, use the following sequence:

| Task                                                                                                     | UI Steps                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Delete the forward list map                                                                              | <ol style="list-style-type: none"> <li>1. On the left navigation pane, go to <b>Inventory</b>  from <b>Traffic</b> and select <b>Maps &gt; Maps &gt; Map</b>.</li> <li>2. Select the forward list map.</li> <li>3. Click Delete.</li> </ol>                                                   |
| Delete the GigaSMART Operation                                                                           | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operation(s) &gt; GigaSMART Operation</b>.</li> <li>2. Select the GigaSMART Operation.</li> <li>3. Click Delete.</li> </ol>                                                                                                                             |
| Disassociate the GigaSMART group from the forward list. (You do not need to delete the GigaSMART group.) | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>2. Select the GigaSMART group.</li> <li>3. Click Edit.</li> <li>4. Under GigaSMART Parameters, go the GTP Whitelist and set GTP Whitelist Alias to None.</li> </ol>                                          |
| Destroy (delete) the forward list.                                                                       | <ol style="list-style-type: none"> <li>1. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART GTP Whitelist</b>.</li> <li>2. Select the GTP Whitelist.</li> <li>3. Click Delete.</li> <li>4. Alternatively ,select the forward list and click on edit option then select the '<b>Clear</b>' radio button, to remove existing forward list.</li> </ol> |

## GTP Whitelisting in a Cluster

The forward list(all whitelist files) must reside on the leader of the cluster. The member nodes receive a copy of the forward list from the leader. Updates to the forward list are synchronized from the leader to the member nodes. If a member node leaves the cluster and rejoins, its forward list will be resynchronized.

If there are GigaVUE TA Series nodes in the cluster, they will not receive a copy of the forward list.

### GTP Flow Sampling

GTP flow sampling samples a configured percentage of GTP sessions. GTP flow sampling uses map rules to select subscribers and then forward a percentage of the packets to tool ports.

Pass rules are defined in flow sampling maps. Each rule contains some combination of IMSI, IMEI, and MSISDN numbers or patterns, Evolved Packet Core (EPC) interface type, GTP version, Access Point Name (APN), or QoS Class Identifier (QCI), as well as a percentage to sample. The flow is sampled to see if it matches a rule. The percentage of the subscriber sessions matching each rule are selected.

Map rules specify the type of traffic to be flow sampled by that map. For each new session, map rules are evaluated in top-down order of decreasing priority. If there is a match, the indicated percentage of the subscriber session is either accepted or rejected. If accepted, the traffic is sent to the tool port or load balancing group specified in the map. If rejected, the traffic is dropped. If there is not a match to a rule, the traffic is passed to subsequent maps.

Starting in software version 4.6, GTP load balancing in a cluster is supported for GTP flow sampling. For an example of GTP load balancing in a cluster, refer to [GigaSMART GTP Whitelisting and GTP Flow Sampling Examples](#).

## About Flow Sampling Rules and Maps

Flow sampling rules are configured in maps called flow sampling maps. Up to ten (10) flow sampling maps per GigaSMART group are supported. Each flow sampling map supports up to 20 flow sampling rules, for a maximum of 200 rules per GigaSMART group.

GTP flow sampling (rule-based flow sampling) is performed after GTP forward list-based forwarding but before GTP flow filtering. So, flow sampling maps have a priority lower than whitelist maps and higher than flow filtering maps.

**NOTE:** For GTP second level maps, a maximum of fifteen maps can be attached to a vport. For example, for the same vport you can have one forward list map and ten flow sampling maps, or ten forward list map, four flow sampling maps, and one flow filtering map. In addition, you can have a collector map, which is not counted.

In the flow sampling maps, the rules in the first map have a higher priority than the rules in the second, third, and subsequent maps. Within any single map, rules are evaluated in order.

Rules can be added to, deleted from, or inserted into a flow sampling map when the subtype selected for a **Second Level** map is **Flow Sample**. Suffix wildcarding, such as IMSI 100\*, is supported in the flow sampling map rules.

Use the **Add a Rule** button in the Maps page to add a new flow sampling rule (a pass rule). Specify IMSI, IMEI, or MSISDN subscriber IDs, as well as the percentage of the flow to be sampled. The percentage is a range from 1 to 100%. Use 0% to drop sampled data.

A rule can specify other packet attributes, such as an EPC interface type or GTP version. An APN pattern can also be specified in a rule, either by itself or preceding the EPC interface or GTP version. A QCI value can be specified, but only in combination with an APN pattern.

EPC interface and GTP version are mutually exclusive. They can be specified in a flow sampling rule, but not both in a single rule. The supported interface types for filtering are: Gn/Gp, S11/S1-U, S5/S8, S10, or S2B. The supported versions for filtering are 1 or 2. For example, you can send version 1 traffic to one tool port and version 2 traffic to another tool port. For more information on interfaces, refer to [Supported Interfaces](#).

For APN, specify a pattern (a name) to match, for example, three.co.uk. Wildcard prefixes and suffixes are supported, for example, \*mobile.com or \*ims\*. The pattern can be specified in up to 100 case-insensitive alphanumeric characters and can include the following special characters: period (.), hyphen (-), and wildcard (\*).

QCI is a mechanism used in Long Term Evolution (LTE) networks to ensure bearer traffic is allocated to the appropriate Quality of Service (QoS). For QCI, specify a value from 0 to 255. Wildcard prefixes and suffixes are not supported.

Use APN and QCI to send traffic that matches a certain APN pattern or that belongs to a certain bearer with a certain QCI to specified tool ports, based on the sampling percentage.

Click the **x** next to a rule to delete a specific rule. Rules are identified by a priority ID, which indicates the order of rules in a flow sampling map. For example, if a map has 12 pass flow sampling rules, there will be 12 priority IDs.

When creating Flow Sampling rules on the Maps page, the first rule created has the highest priority and the priority of subsequent rules is in the order that they are added. To change the priority of a Flow Sampling rule in a new map, do the following:

1. **Save** the rule.
2. Select the map and click **Edit**.
3. Enter a priority in the **Priority** field of each rule to order the rules in the map. (For details about map priority, refer to [Map Priority](#))

**NOTE:** A flow sampling map can contain only flowsampling rules. A flow sampling map cannot contain other GigaSMART rules (gsrule) or flow filtering rules (flowrule).

For configuration examples for flow sampling, refer to [GigaSMART GTP Whitelisting and GTP Flow Sampling Examples](#).

## Add Rule to Flow Sampling Map

Flow sampling is applied for new subscribers. When a new rule is added to the rules in a flow sampling map, traffic will be sent to the port or load balancing group specified in the map.G

## Delete Rule from a Flow Sampling Map

When a rule is deleted from a flow sampling map, the session associated with the rule stays active. The traffic associated with the rule will not be reevaluated by subsequent maps.

## Change Priority of Flow Sampling Maps

Use the **Priority** field in the GTP map rule to set the priority of flow sampling maps.

**NOTE:** Editing the map priority in non-overlap will reset the active sessions. Total sessions will remain unaffected and continue incrementing with incoming user traffic.

## Delete Flow Sampling Map

When a flow sampling map is deleted, the priority of the remaining flow sampling maps will be re-prioritized. For example, if the first flow sampling map is deleted, the second flow sampling map will increase in priority.

For the deleted flow sampling map, the traffic associated with the rules in the map will be reevaluated and then passed to subsequent maps.

When a flow sampling map is re-prioritized, the existing sessions will be reevaluated according to the new priority of the map. The traffic associated with the rules in the map will be reevaluated and then passed to subsequent maps.

When the last flow sampling map is deleted, the traffic associated with the rules in the map will also be reevaluated before being passed to subsequent maps. But the traffic associated with the rules in maps that were not matched, will not be reevaluated because that traffic was already passed to subsequent maps.

## Flow-Ops Report Limitation for Multiple Flow Sampling Maps

The flow-ops report displays the flow sampling rule ID for sessions that have been accepted or rejected by the flow sampling map.

However, since rule IDs are not unique across maps, when there are multiple flow sampling maps, the flow-ops report is unable to identify the exact rule that the session matched. For example, with multiple flow sampling maps, each map can have a rule ID of 1. The rule ID will be identified in the flow-ops report, but not the map associated with it.

## GTP Flow Sampling Percentage

The sampling Percentage field in a map for GTP flow sampling, represents the percentage of subscribers that will be sampled (not the sessions).

The GTP correlation engine tracks all of the subscribers and all of their sessions that it sees on the network. In this example, for those subscribers with an IMSI starting with the value 46\*, the GTP correlation engine keeps a list of them and randomly selects 80% of those subscribers and sets them to be in the sample, which means that a tool port (or load balanced group) will see 100% of the packets for 100% of the sessions for those randomly selected 80% of subscribers.

For the other 20% of subscribers, the GTP correlation engine continuously tracks those subscribers through the network, but does not send any packets to the tool port (or load balanced group).

Refer to the GTP flow sampling configuration examples in [Required Licenses: GTP Filtering & Correlation and FlowVUE](#).

## Drop Unmatched Traffic

When a session matches one of the configured flow sampling rules, it is either accepted for sampling or rejected.

If it is accepted, all packets belonging to that GTP session are sent to the tool port or ports specified in the flow sampling maps. If a subscriber is in the sample, then both the control plane packets and the user-data plane packets are sent to the tools.

If it is rejected, all packets belonging to the session are dropped. If the subscriber is not in the sample, then neither the control plane packets nor the user-data plane packets are sent to the tools.

Control plane (GTP-c) and user-data plane (GTP-u) traffic are treated the same. For a matching session, all the control plane and user-data plane traffic will be accepted. Otherwise, all the control plane and user-data plane traffic will be rejected and dropped. Instead, to enable or disable GTP control plane traffic sampling, refer to [Enable or Disable GTP Control Plane Traffic Sampling](#).

## Enable or Disable GTP Control Plane Traffic Sampling

GTP control plane (GTP-c) traffic is typically a small percentage of total GTP traffic, but it contains useful information for analytics. Therefore, it is not always expedient to drop control plane traffic for sampled sessions.

Subscriber traffic by IMSI can be sampled such that network traffic for a subset of mobile subscribers can be selected to be sent to network monitoring tools. In some cases, network monitoring tools will want to see GTP control plane and GTP user plane traffic for a percentage of the subscribers. In other cases, network monitoring tools will want to see all of the GTP control plane traffic, but see only the GTP user plane traffic for the sampled percentage of subscribers.

Starting in software version 4.5, all control plane traffic for all subscribers will be sent to tools if GTP control plane traffic sampling is disabled. When disabled, 100% of the control traffic that matches any of the flow sampling rules will be sent to the tool ports specified in the flow sampling maps. Control traffic for both accepted and rejected sessions will be sent to the tool ports.

When GTP control plane traffic sampling is enabled, GTP-c packets will be sampled and only the indicated percentage of the control traffic that matches any of the flow sampling rules will be sent to the tool ports specified in the flow sampling maps, as described in [GTP Flow Sampling Percentage](#).

The default is enable.

To disable sampling of GTP-c traffic, which enables 100% of control plane traffic, select **GigaSMART > GigaSMART Groups > GigaSMART Groups**. Under GigaSMART Parameters, go to **GTP Sampling** and make sure that **GTP Control Sampling** is not selected.

To enable sampling of GTP-c traffic, which enables 100% of control plane traffic, select **GigaSMART > GigaSMART Groups > GigaSMART Groups**. Under GigaSMART Parameters, go to **GTP Sampling** and make sure that **GTP Control Sampling** is selected. This setting applies to all the flow sampling maps for a GigaSMART group.

### GTP Subscriber Aware Random Sampling

GTP Subscriber Aware Random Sampling allows to randomly sample all the subscriber's IMSI on a rotational basis. Based on the configured sampling percentage, the selected sessions are either sampled in or out. The correlation engine takes the configurable interval as an input to rotate the random selection of each of the subscriber's sessions.

The configurable interval is a minimum of 12 hours and a maximum of 48 hours. Each GigaSMART node must be synchronized with an NTP/PTP server, as UTC time is involved in the random selection of the subscriber's sessions.

**NOTE:** This feature is effective for a new subscriber's sessions after enabling the random sampling.

The Map rules in the GTP random sampling are similar to GTP Flow Sampling. For more information refer to [GigaSMART GTP Whitelisting and GTP Flow Sampling](#).

To enable GTP Random Sampling do the following:

1. From the left navigation pane, go to **System > GigaSMART > GigaSMART Groups**.
2. Select a GigaSMART Group and click **Edit**.
3. Under GigaSMART Parameters, go to **GTP** and select **GTP Random Sampling** check box.
4. Enter the time in **Rotation Interval in multiples of 12 hours**.
5. Click **OK**.

## Display GTP Flow Ops Report Statistics

To display GTP statistics, select **GigaSMART > GigaSMART Operations (GSOP) > Statistics**.

Refer to [Flow Ops Report Statistics Definitions for GTP on page 635](#) for descriptions of these statistics.

### GigaSMART GTP Whitelisting and GTP Flow Sampling Examples

Refer to the following examples:

- [Example 1: GTP Whitelisting](#)
- [Example 2: GTP Whitelisting with Multiple Maps](#)
- [Example 3: GTP Flow Sampling](#)
- [Example 4: GTP Whitelisting, GTP Flow Sampling, and Load Balancing](#)
- [Example 5: GTP Flow Sampling with Multiple Maps](#)
- [Example 6: APN for GTP Whitelisting, GTP Flow Sampling](#)
- [Example 7: APN for FTP Whitelisting, APN and QCI for GTP Flow Sampling](#)

### Example 1: GTP Whitelisting

Example 1 is a GTP whitelisting configuration example. Traffic from network ports go to the three first level maps (GTP-Control, GTP-User, and Fragments-Not\_First) and then to the virtual port (vport1). If there is a match to an IMSI in the whitelist (MyIMSI), it is forwarded to a port.

| Task | Description                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure a GigaSMART group and associate it with a GigaSMART engine port.     | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups</b>.</li> <li>Click New.</li> <li>Type an alias in the Alias field and enter an engine port in the Port List field.</li> <li>Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                          |
| 2.   | Create a virtual port.                                                         | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</li> <li>Click New.</li> <li>Type an alias in the Alias field and enter an engine port in the Port List field.</li> <li>From the GigaSMART Groups drop-down list, select the GigaSMART group created in task 1.</li> <li>Click Save.</li> </ul>                                                                                                                                                                                                            |
| 3.   | Create the GTP whitelist.                                                      | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GTP Whitelist</b>.</li> <li>Click New.</li> <li>Type an alias in the Alias field. You can also create multiple whitelist aliases per gsgroup during the creation of solution.</li> <li>From the GigaSMART Groups drop-down list, select the GigaSMART group created in Task 1.</li> <li>Go to Task 4.</li> </ul>                                                                                                                                                              |
| 4.   | Fetch whitelist files from a specified location to populate the GTP whitelist. | <ul style="list-style-type: none"> <li>On the GTP Whitelist page, select Bulk Upload.</li> <li>Select Bulk Entry Operation for IMSI Upload Type</li> <li>Select Upload from URL from the Bulk Upload Type list.</li> <li>Enter the URL in the Enter Remote URL field. For example, <a href="http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx">http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx</a></li> <li>Click Save.</li> </ul>                                                                                                                                                 |
| 5    | Associate the GigaSMART group to the GTP whitelist.                            | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups</b>.</li> <li>Select the GigaSMART Group created in Task 1 and click Edit.</li> <li>Type an alias in the Alias field. You can also associate multiple whitelist aliases per gsgroup during the creation of solution.</li> <li>From the GigaSMART Groups drop-down list, select the GigaSMART group created in task 1.</li> <li>Under GTP Whitelist, click on the GTP Whitelist Alias field and select the alias from Task 3.</li> <li>Click Save.</li> </ul> |
| 6.   | Configure the GigaSMART operation for GTP whitelisting.                        | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations &gt; GigaSMART Operation</b>.</li> <li>Click New.</li> <li>Type an alias in the Alias field. For example, GTP-Whitelist.</li> <li>Select the GigaSMART group created in task 1.</li> </ul>                                                                                                                                                                                                                                                               |

| Task | Description                                                                                                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                            | <ul style="list-style-type: none"> <li>From the GigaSMART Operations (GSOP) drop-down list, select the following: <ul style="list-style-type: none"> <li>GTP Whitelist and select Enabled.</li> <li>Load Balancing.</li> </ul> </li> <li>For Load Balancing, do the following: <ul style="list-style-type: none"> <li>Choose Stateful</li> <li>For Type select GTP</li> </ul> </li> <li>Choose Hashing for the metric and select IMSI</li> <li>Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 7.   | <p>Configure three first level maps.</p> <div> <p><b>NOTE:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.</p> </div>                   | <ul style="list-style-type: none"> <li>Configure the first map as follows: <ul style="list-style-type: none"> <li>Alias: GTP-Control</li> <li>Type and subtype: First Level By Rule</li> <li>Source: network port or ports</li> <li>Destination: virtual port created in Task 2.</li> <li>Rule: Pass, Bi Directional, Port Destination 2123</li> <li>Map Permissions: Select current user's group for Owner</li> <li>Save the map</li> </ul> </li> <li>Configure the second map as follows: <ul style="list-style-type: none"> <li>Alias: GTP-User</li> <li>Type and subtype: First Level By Rule</li> <li>Source: Same network port or ports as first map.</li> <li>Destination: virtual port created in Task 2.</li> <li>Rule: Pass, Bi Directional, Port Destination 2152</li> <li>Map Permissions: Select current user's group for Owner</li> <li>Save the map</li> </ul> </li> <li>Configure the third map as follows: <ul style="list-style-type: none"> <li>Alias: Fragments-Not-First</li> <li>Type and subtype: First Level By Rule</li> <li>Source: Same network port or ports as first map</li> <li>Destination: virtual port created in Task 2</li> <li>Rule: Pass, IPv4 Fragmentation and select allFragNoFirst</li> <li>Map Permissions: Select current user's group for Owner.</li> <li>Save the map</li> </ul> </li> </ul> |
| 8.   | Configure a second level map for GTP whitelisting, the whitelist map. If there is a match to an IMSI in the whitelist (MyIMSI), it is forwarded to a port. | <ul style="list-style-type: none"> <li>Configure the second level map as follows: <ul style="list-style-type: none"> <li>Alias: GTP-Whitelist</li> <li>Type and subtype: Second Level By Rule</li> <li>Source: virtual port created in Task 2</li> <li>Destination: select a tool port</li> <li>GSOP: GigaSMART Operation created in Task 6</li> <li>Map Permissions: Select current user's group for Owner</li> </ul> </li> <li>Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Example 2: GTP Whitelisting with Multiple Maps

Example 2 is a GTP whitelisting configuration example that includes multiple GTP whitelisting maps, which provide a more granular selection of tool ports.

Traffic from network ports go to the three first level maps (GTP-Control, GTP-User, and Fragments-Not-First) and then to the virtual port (vport1). Two whitelist maps are configured. The first map specifies a rule for version 1 traffic. The second map specifies a rule for version 2 traffic.

| Task | Description                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                           |
|------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure a GigaSMART group and associate it with a GigaSMART engine port.     | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>Click New.</li> <li>Type an gsg1 in the Alias field and enter an engine port in the Port List field, for example 10/7/e1.</li> <li>Click Save.</li> </ul>                                                            |
| 2.   | Create a virtual port.                                                         | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</li> <li>Click New.</li> <li>Type vport1 in the Alias field.</li> <li>From the GigaSMART Groups drop-down list, select the GigaSMART group created in task 1.</li> <li>Click Save.</li> </ul>                                                          |
| 3.   | Create the GTP whitelist.                                                      | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GTP Whitelist</b>.</li> <li>Click New.</li> <li>Type an MyIMSI in the Alias field.</li> <li>From the GigaSMART Groups drop-down list, select the GigaSMART group created in Task 1.</li> <li>Go to Task 4.</li> </ul>                                                     |
| 4.   | Fetch whitelist files from a specified location to populate the GTP whitelist. | <ul style="list-style-type: none"> <li>On the GTP Whitelist page, select Bulk Upload.</li> <li>Select Bulk Entry Operation for IMSI Upload Type</li> <li>Select Upload from URL from the Bulk Upload Type list.</li> <li>Enter the URL in the Enter Remote URL field. For example, <code>http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx</code></li> <li>Click Save.</li> </ul> |
| 5.   | Associate the GigaSMART group to the GTP whitelist.                            | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>Select the GigaSMART Group created in Task 1 and click Edit.</li> <li>From the GigaSMART Groups drop-down list, select the</li> </ul>                                                                                |

| Task | Description                                                                                                                              | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                          | <p>GigaSMART group created in task 1.</p> <ul style="list-style-type: none"> <li>Under GTP Whitelist, click on the GTP Whitelist Alias field and select the alias from Task 3.</li> <li>Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 5.   | Configure the GigaSMART operation for GTP whitelisting.                                                                                  | <ul style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations &gt; GigaSMART Operation</b>.</li> <li>Click New.</li> <li>Type gtp-whitelist in the Alias field.</li> <li>Select the GigaSMART group created in task 1.</li> <li>From the GigaSMART Operations (GSOP) drop-down list, select the following: <ul style="list-style-type: none"> <li>GTP Whitelist and select Enabled.</li> <li>Load Balancing.</li> </ul> </li> <li>For Load Balancing, do the following: <ul style="list-style-type: none"> <li>Choose Stateful</li> <li>For Type select GTP</li> <li>Choose Hashing for the metric and select IMSI</li> <li>Click Save.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                              |
| 6.   | <p>Configure three first level maps.</p> <div> <p><b>NOTE:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.</p> </div> | <p>Configure the first map.</p> <ol style="list-style-type: none"> <li>On the left navigation pane, go to <b>Inventory</b>  from <b>Traffic</b> and select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>Click New.</li> <li>Configure the map: <ul style="list-style-type: none"> <li>Alias: GTP-Control</li> <li>Type: First Level, Sub Type: By Rule</li> <li>Source: 8/1/x40, 8/1/x6</li> <li>Destination: vport1</li> </ul> </li> <li>Click Add a Rule. <ul style="list-style-type: none"> <li>Select Pass and Bi Directional</li> <li>Select Port Destination for the rule</li> <li>Set port value to 2123</li> </ul> </li> <li>Click Save.</li> </ol> <ul style="list-style-type: none"> <li>Configure the second map. <ol style="list-style-type: none"> <li>Click New.</li> <li>Configure the map: <ul style="list-style-type: none"> <li>Alias: GTP-User</li> <li>Type: First Level, Sub Type: By Rule</li> <li>Source: 8/1/x40, 8/1/x6</li> <li>Destination: vport1</li> </ul> </li> <li>Click Add a Rule.</li> </ol> </li> </ul> |

| Task | Description                                                                                                                                                                                                      | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>■ Select Pass and Bi Directional</li> <li>■ Select Port Destination for the rule</li> <li>■ Set port value to 2152</li> <li>d. Click Save.</li> </ul> <ul style="list-style-type: none"> <li>• Configure the second map.               <ul style="list-style-type: none"> <li>a. Click New.</li> <li>b. Configure the map:                   <ul style="list-style-type: none"> <li>■ Alias: Fragment-Not-First</li> <li>■ Type: First Level, Sub Type: By Rule</li> <li>■ Source: 8/1/x40, 8/1/x6</li> <li>■ Destination: vport1</li> </ul> </li> <li>c. Click Add a Rule.                   <ul style="list-style-type: none"> <li>■ Select Pass</li> <li>■ Select Port IPv4 Fragmentation for the rule</li> <li>■ Select allFragNoFirst for Value</li> </ul> </li> <li>d. Click Save.</li> </ul> </li> </ul> |
| 7.   | Configure one second level map for GTP whitelisting, the first whitelist map. If there is a match to version 1 and if the IMSI is present in the whitelist (MyIMSI), it is forwarded to the specified port.      | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New.</li> <li>c. Configure the map:               <ul style="list-style-type: none"> <li>■ Alias: GTP-Whitelist_v1</li> <li>■ Type: Second Level, Sub Type: Flow Whitelist</li> <li>■ Source: vport1</li> <li>■ Destination: 1/2x23</li> <li>■ Select gtp-whitelist from the GSOP list.</li> </ul> </li> <li>d. Click Add a Rule.               <ul style="list-style-type: none"> <li>■ Select GTP</li> <li>■ Set Version to V1</li> </ul> </li> <li>e. Click Save.</li> </ul>                                                                                                    |
| 8.   | Configure another second level map for GTP whitelisting, the second whitelist map. If there is a match to version 2 and if the IMSI is present in the whitelist (MyIMSI), it is forwarded to the specified port. | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New.</li> <li>c. Configure the map:               <ul style="list-style-type: none"> <li>■ Alias: GTP-Whitelist_v2</li> <li>■ Type: Second Level, Sub Type: Flow Whitelist</li> <li>■ Source: vport1</li> <li>■ Destination: 1/2x24</li> <li>■ Select gtp-whitelist from the GSOP list.</li> </ul> </li> <li>d. Click Add a Rule.</li> </ul>                                                                                                                                                                                                                                     |

| Task | Description | UI Steps                                                                                                          |
|------|-------------|-------------------------------------------------------------------------------------------------------------------|
|      |             | <ul style="list-style-type: none"> <li>■ Select GTP</li> <li>■ Set Version to V2</li> </ul> <p>e. Click Save.</p> |

### Example 3: GTP Flow Sampling

Example 3 is a GTP flow sampling configuration example. Traffic from network ports go to the three first level maps (GTP-Control, GTP-User, and Fragments-Not\_First) and then to the virtual port (vport1). The traffic flow is sampled based on the rules in one flow sampling map (GTP-Sample-01). The flow sampling rules specify IMSI, IMEI, and MSISDN numbers, as well as the percentage to sample. Packets are then accepted or rejected. Accepted packets are forwarded to a port. Rejected packets are dropped. Packets that do not match a rule will be passed to subsequent maps.

| Task | Description                                                                                                                                                                                              | UI Steps                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure a GigaSMART group and associate it with a GigaSMART engine port.                                                                                                                               | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</p> <p>b. Click New.</p> <p>c. Type an alias in the Alias field and enter an engine port in the Port List field.</p> <p>d. Click Save.</p>                                                                                                                                        |
| 2.   | Create a virtual port.                                                                                                                                                                                   | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</p> <p>b. In the Alias field, type an alias for this virtual port.</p> <p>c. Type an alias in the Alias field and enter an engine port in the Port List field.</p> <p>d. From the GigaSMART Groups drop-down list, select the GigaSMART group created in task 1.</p> <p>e. Click Save.</p>                 |
| 3.   | Configure three first level maps.<br><div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <b>NOTE:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.           </div> | <p>a. Configure the first map as follows:</p> <ul style="list-style-type: none"> <li>■ Alias: GTP-Control</li> <li>■ Type and subtype: First Level By Rule</li> <li>■ Source: network port or ports</li> <li>■ Destination: virtual port created in Task 2.</li> <li>■ Rule: Pass, Bi Directional, Port Destination 2123</li> <li>■ Map Permissions: Select current user's group for Owner</li> </ul> |

| Task | Description                                                                                                                            | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                        | <ul style="list-style-type: none"> <li>■ Save the map</li> <li>b. Configure the second map as follows:               <ul style="list-style-type: none"> <li>■ Alias: GTP-User</li> <li>■ Type and subtype: First Level By Rule</li> <li>■ Source: Same network port or ports as first map.</li> <li>■ Destination: virtual port created in Task 2.</li> <li>■ Rule: Pass, Bi Directional, Port Destination 2152</li> <li>■ Map Permissions: Select current user's group for Owner</li> <li>■ Save the map</li> </ul> </li> <li>c. Configure the third map as follows:               <ul style="list-style-type: none"> <li>■ Alias: Fragments-Not-First</li> <li>■ Type and subtype: First Level By Rule</li> <li>■ Source: Same network port or ports as first map</li> <li>■ Destination: virtual port created in Task 2</li> <li>■ Rule: Pass, IPv4 Fragmentation and select allFragNoFirst</li> <li>■ Map Permissions: Select current user's group for Owner</li> </ul> </li> <li>d. Save the map</li> </ul> |
| 4.   | Configure the GigaSMART operation for GTP flow sampling.                                                                               | <ul style="list-style-type: none"> <li>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operations</b>.</li> <li>b. Click New.</li> <li>c. Type an alias in the Alias field. For example, GTP-Whitelist.</li> <li>d. Select the GigaSMART group created in task 1.</li> <li>e. From the GigaSMART Operations (GSOP) drop-down list, select the following:               <ul style="list-style-type: none"> <li>■ GTP Whitelist and select Enabled.</li> <li>■ Load Balancing.</li> </ul> </li> <li>f. For Load Balancing, do the following:               <ul style="list-style-type: none"> <li>a. Choose Stateful</li> <li>b. For Type select GTP</li> <li>c. Choose Hashing for the metric and select IMSI</li> </ul> </li> <li>d. Click Save.</li> </ul>                                                                                                                                                                                     |
| 5.   | Configure a second level map for GTP flow sampling, the flow sampling map. The traffic flow is sampled based on the rules in this map. | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New.</li> <li>c. Configure the map.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Task | Description | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |             | <ul style="list-style-type: none"> <li>■ Type GTP-Sample-01 in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype.</li> <li>■ Select the virtual port configured in Task 2 for the Source</li> <li>■ Select a tool port for the Destination</li> <li>■ Select the GigaSMART Operation configured in Task 4 for from the GSOP list</li> </ul> <p>d. Use the Add a Rule button to create the following flow sampling rules:</p> <ul style="list-style-type: none"> <li>■ Percentage to 50, IMEI 01416800*</li> <li>■ Percentage to 80, IMSI 46*</li> <li>■ Percentage to 25, MSISDN 1509*</li> <li>■ Percentage to 15, IMSI 01400*</li> <li>■ Percentage to 20, IMSI, 31*, MSISDN 1909*</li> </ul> <p>e. Click Save.</p> |

## Example 4: GTP Whitelisting, GTP Flow Sampling, and Load Balancing

Example 4 combines the GTP whitelisting configuration from Example 1 with the GTP flow sampling configuration from Example 3, and adds GigaSMART load balancing.

In Example 4, traffic from network ports go to the three first level maps (GTP-Control, GTP-User, and Fragments-Not-First) and then to the virtual port (vport1). If there is a match to an IMSI in the whitelist (MyIMSI), it is forwarded to the port group (PG-Whitelist) for load balancing.

**NOTE:** In Example 4, the tool ports in the port group are on the same node as the GigaSMART group and GigaSMART operation.

If there is not a match to an IMSI in the whitelist, the traffic flow is sampled based on the rules in the flow sampling map (GTP-Sample-01). The flow sampling rules specify IMSI, IMEI, and MSISDN numbers, as well as the percentage to sample. Packets are then accepted or rejected. Accepted packets are forwarded to the port group (PG-Sample) for load balancing. Rejected packets are dropped. Packets that do not match a rule will be passed to subsequent maps.

| Task | Description                                                   | UI Steps                                                                                   |
|------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1.   | Create port groups and specify the tool ports and enable load | a. Go to <b>System &gt; Ports &gt; select Ports &gt; Port Groups &gt; All Port Groups.</b> |

| Task | Description                                                                                                                                                                                        | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | balancing.                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>b. Click New.</li> <li>c. Type PG-Whitelist in the Alias field.</li> <li>d. Select SMART Load Balancing</li> <li>e. Click in the Ports field and select the tool ports for the port group.</li> <li>f. Click Save.</li> <li>g. Repeat steps 2 through 6, to create a port group with the alias PF-Sample.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 2.   | Configure a GigaSMART group and associate it with a GigaSMART engine port.                                                                                                                         | <ul style="list-style-type: none"> <li>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>b. Click New.</li> <li>c. Type an alias in the Alias field and enter an engine port in the Port List field.</li> <li>d. Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 3.   | Create a virtual port.                                                                                                                                                                             | <ul style="list-style-type: none"> <li>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</li> <li>b. In the Alias field, type an alias for this virtual port.</li> <li>c. Type an alias in the Alias field and enter an engine port in the Port List field.</li> <li>d. From the GigaSMART Groups drop-down list, select the GigaSMART group created in task 1.</li> <li>e. Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 4.   | Configure three first level maps. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p><b>NOTE:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.</p> </div> | <ul style="list-style-type: none"> <li>a. Configure the first map as follows:               <ul style="list-style-type: none"> <li>■ Alias: GTP-Control</li> <li>■ Type and subtype: First Level By Rule</li> <li>■ Source: network port or ports</li> <li>■ Destination: virtual port created in Task 2.</li> <li>■ Rule: Pass, Bi Directional, Port Destination 2123</li> <li>■ Map Permissions: Select current user's group for Owner</li> </ul> </li> <li>b. Save the map</li> <li>c. Configure the second map as follows:               <ul style="list-style-type: none"> <li>■ Alias: GTP-User</li> <li>■ Type and subtype: First Level By Rule</li> <li>■ Source: Same network port or ports as first map.</li> <li>■ Destination: virtual port created in Task 2.</li> <li>■ Rule: Pass, Bi Directional, Port Destination 2152</li> <li>■ Map Permissions: Select current user's group for Owner</li> <li>■ Save the map</li> </ul> </li> <li>d. Configure the third map as follows:               <ul style="list-style-type: none"> <li>■ Alias: Fragments-Not-First</li> </ul> </li> </ul> |

| Task | Description                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                | <ul style="list-style-type: none"> <li>■ Type and subtype: First Level By Rule</li> <li>■ Source: Same network port or ports as first map</li> <li>■ Destination: virtual port created in Task 2</li> <li>■ Rule: Pass, IPv4 Fragmentation and select allFragNoFirst</li> <li>■ Map Permissions: Select current user's group for Owner</li> </ul> <p>e. Save the map</p>                                                                                                      |
| 5.   | Create the GTP whitelist.                                                      | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GTP Whitelist</b>.</p> <p>b. Click New.</p> <p>c. Type an Alias for the Whitelist in the Alias field. For example, MyIMSI</p>                                                                                                                                                                                                                                                                         |
| 6.   | Fetch whitelist files from a specified location to populate the GTP whitelist. | <p>a. On the GTP Whitelist page, select Bulk Upload.</p> <p>b. Select Bulk Entry Operation for IMSI Upload Type</p> <p>c. Select Upload from URL from the Bulk Upload Type list.</p> <p>d. Enter the URL in the Enter Remote URL field. For example, http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx</p> <p>e. Click Save.</p>                                                                                                                                             |
| 7.   | (Optional) Add a single IMSI to the GTP whitelist.                             | <p>a. On the GTP Whitelist page, select Individual Entry Operation.</p> <p>b. Select Append for Operation Type</p> <p>c. Enter the IMSI entry in the Individual IMSI Entry field.</p> <p>d. Click Save.</p>                                                                                                                                                                                                                                                                   |
| 8.   | Associate the GigaSMART group to the GTP whitelist.                            | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</p> <p>b. Click New.</p> <p>c. Type an alias in the Alias field.</p> <p>d. Under GTP Whitelist, click on the GTP Whitelist Alias field and select the alias from Task 5.</p> <p>e. Click Save.</p>                                                                                                                                                        |
| 9.   | Configure the GigaSMART operation for GTP whitelisting.                        | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP)&gt; GigaSMART Operation</b>.</p> <p>b. Click New.</p> <p>c. Select the GigaSMART Group created in Task 8 from the GigaSMART Groups list.</p> <p>d. Type an alias in the Alias field. For example, gtp-whitelist.</p> <p>e. Select GTP Whitelist from the GigaSMART Operations (GSOP) list.</p> <p>f. Select Load Balancing from the GigaSMART Operations (GSOP) list.</p> |

| Task | Description                                                                                                                                                                     | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>g. Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMSI</li> </ul> </li> <li>h. Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 10.  | Configure a second level map for GTP whitelisting, the whitelist map. If there is a match to an IMSI in the whitelist (MyIMSI), it is forwarded to a load balancing port group. | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New</li> <li>c. Configure the map. <ul style="list-style-type: none"> <li>■ Type an name in the Alias field. For example GTP-Whitelist.</li> <li>■ Select Second Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Select the GigaSMART Operation configured in Task 9 from the GigaSMART Operations (GSOP) list.</li> <li>■ Select the virtual port configured in Task 3 for Source</li> <li>■ Select PG-Whitelist for Destination</li> </ul> </li> <li>d. Click Save.</li> </ul> |
| 11.  | Configure the GigaSMART operation for GTP flow sampling.                                                                                                                        | <ul style="list-style-type: none"> <li>e. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP) &gt; GigaSMART Operation</b>.</li> <li>f. Click New.</li> <li>g. Select the GigaSMART Group created in Task 8 from the GigaSMART Groups list.</li> <li>h. Type an alias in the Alias field. For example, gtp-flowsample.</li> <li>i. Select Flow Sampling from the GigaSMART Operations (GSOP) list.</li> <li>j. Select Flow Sampling-GTP.</li> <li>k. Select Load Balancing from the GigaSMART Operations (GSOP) list. <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMSI</li> </ul> </li> <li>l. Click Save.</li> </ul>                  |
| 12.  | Configure a second level map for GTP flow sampling, the flow sampling map. If there is not a match to an IMSI in the whitelist,                                                 | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New</li> <li>c. Configure the map.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Task | Description                                                                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | the traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to a load balancing port group. | <ul style="list-style-type: none"> <li>■ Type an name in the Alias field. For example GTP-Sample-01.</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype</li> <li>■ Select the GigaSMART operation for flow sampling configured in Task 11 from the GSOP list.</li> <li>■ Select the virtual port configured in Task 3 for Source</li> <li>■ Select PG-Sample for Destination</li> </ul> <p>d. Create the following flow sample rules:</p> <ul style="list-style-type: none"> <li>■ Percentage 50, IMEI 01416800*, IMSI 31*</li> <li>■ Percentage 80, IMSI 46*</li> <li>■ Percentage 25, MSISDN 1509*</li> <li>■ Percentage 15, IMEI 01400*, imsi 31*</li> <li>■ Percentage 20, IMSI 31*, MSISDN 1909*</li> </ul> <p>e. Click Save.</p> |

## Example 5: GTP Flow Sampling with Multiple Maps

Example 5 includes multiple GTP flow sampling maps, which provide a more granular selection of tool ports for flow sampling.

In Example 5, traffic from network ports go to the three first level maps (GTP-Control, GTP-User, and Fragments-Not\_First) and then to the virtual port (vport1). If there is a match to an IMSI in the whitelist (VoLTE\_1MM), it is forwarded to the port-group (PG-Whitelist-1) for load balancing.

**NOTE:** In Example 5, the tool ports in the port group are on the same node as the GigaSMART group and GigaSMART operation.

If there is not a match to an IMSI in the whitelist, the traffic flow is sampled based on the rules in the four flow sampling maps (GTP-Sample-1 to GTP-Sample-4).

The flow sampling rules in each map specify IMSI, IMEI, and MSISDN numbers, as well as the percentage to sample. Packets are then accepted or rejected. Accepted packets are forwarded to the port-group (PG-Sample-1 to PG-Sample-4) for load balancing. Rejected packets are dropped. Packets that do not match a rule will be passed to subsequent maps, in this example, to a shared collector.

| Task | Description                    | UI Steps                                                                      |
|------|--------------------------------|-------------------------------------------------------------------------------|
| 1.   | Create port groups, specifying | a. Go to <b>System &gt; Ports &gt; select Ports &gt; Port Groups &gt; All</b> |

| Task | Description                                                                                                      | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | the tool ports and enabling load balancing.                                                                      | <p><b>Port Groups.</b></p> <ol style="list-style-type: none"> <li>Click New.</li> <li>Type PG-Sample-1 in the Alias field.</li> <li>Select SMART Load Balancing</li> <li>Click in the Ports field and select the tool ports for the port group.</li> <li>Click Save.</li> <li>Repeat steps 2 through 6, to create a port groups with the aliases</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 2.   | Configure a GigaSMART group and associate it with a GigaSMART engine port.                                       | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups.</b></li> <li>Click New.</li> <li>Type an alias in the Alias field and enter an engine port in the Port List field.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 3.   | Create a virtual port.                                                                                           | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports.</b></li> <li>Type vport1 in the Alias field.</li> <li>Select the GigaSMART Groups created in Task 2 from the GigaSMART Group list.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 4.   | Configure three first level maps.<br><b>Note:</b> In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic. | <ol style="list-style-type: none"> <li>Configure the first map as follows:               <ul style="list-style-type: none"> <li>Alias: GTP-Control</li> <li>Type and subtype: First Level By Rule</li> <li>Source: network ports (for example, 10/1/x5, 10/3/x1, 10/6/q1)</li> <li>Destination: virtual port created in Task 2.</li> <li>Rule: Pass, Bi Directional, Port Destination 2123</li> <li>Save the map</li> </ul> </li> <li>Configure the second map as follows:               <ul style="list-style-type: none"> <li>Alias: GTP-User</li> <li>Type and subtype: First Level By Rule</li> <li>Source: Same network ports as first map.</li> <li>Destination: virtual port created in Task 2.</li> <li>Rule: Pass, Bi Directional, Port Destination 2152</li> <li>Save the map</li> </ul> </li> <li>Configure the third map as follows:               <ul style="list-style-type: none"> <li>Alias: Fragments-Not-First</li> <li>Type and subtype: First Level By Rule</li> <li>Source: Same network ports as first map</li> </ul> </li> </ol> |

| Task | Description                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                | <ul style="list-style-type: none"> <li>■ Destination: virtual port created in Task 2</li> <li>■ Rule: Pass, IPv4 Fragmentation and select allFragNoFirst</li> </ul> <p>d. Save the map</p>                                                                                                                                                                                                                                                                                                                   |
| 5.   | Create the GTP whitelist.                                                      | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GTP Whitelist</b>.</p> <p>b. Click New.</p> <p>c. Enter VoLTE_1MM in the Alias field.</p> <p>d. Go to Task 6.</p>                                                                                                                                                                                                                                                                                                                    |
| 6.   | Fetch whitelist files from a specified location to populate the GTP whitelist. | <p>a. On the GTP Whitelist page, select Bulk Upload.</p> <p>b. Select Bulk Entry Operation for IMSI Upload Type</p> <p>c. Select Upload from URL from the Bulk Upload Type list.</p> <p>d. Enter the URL in the Enter Remote URL field. For example, <a href="http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx">http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx</a></p> <p>e. Click Save.</p>                                                                                                           |
| 7.   | (Optional) Add a single IMSI to the GTP whitelist.                             | <p>a. On the GTP Whitelist page, select Individual Entry Operation.</p> <p>b. Select Append for Operation Type</p> <p>c. Enter the IMSI entry in the Individual IMSI Entry field.</p> <p>d. Click Save.</p>                                                                                                                                                                                                                                                                                                  |
| 8.   | Associate the GigaSMART group to the GTP whitelist.                            | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b></p> <p>b. Click New.</p> <p>c. Type gsg1 in the Alias field.</p> <p>d. Under GTP Whitelist, click on the GTP Whitelist Alias field and select VoLTE_1MM.</p> <p>e. Click Save.</p>                                                                                                                                                                                                        |
| 9.   | Configure the GigaSMART operation for GTP whitelisting.                        | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP) &gt; GigaSMART Operation</b>.</p> <p>b. Click New.</p> <p>c. Select the GigaSMART Group gsg1 created in Task 8 from the GigaSMART Groups list.</p> <p>d. Enter gtp-whitelistl in the Alias field.</p> <p>e. Select GTP Whitelist from the GigaSMART Operations (GSOP) list</p> <p>f. Select Load Balancing from the GigaSMART Operations (GSOP) list.</p> <p>g. Configure Load Balancing as follows:</p> |

| Task | Description                                                                                                                                                                        | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMSI</li> </ul> <p>h. Click Save.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 10.  | Configure a second level map for GTP whitelisting, the whitelist map. If there is a match to an IMSI in the whitelist (VoLTE_1MM), it is forwarded to a load balancing port group. | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click New</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Enter GTP-Whitelist in the Alias field.</li> <li>■ Select Second Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Select gtp-whitelist from the GSOP list.</li> <li>■ Select the virtual port vport1 configured in Task 3 for Source</li> <li>■ Select port group PG-Whitelist-2 for Destination</li> </ul> <p>d. Click Save.</p>                                                                   |
| 11.  | Configure the GigaSMART operation for GTP flow sampling.                                                                                                                           | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation</b>.</p> <p>b. Click New.</p> <p>c. Select the GigaSMART Group created in Task 8 from the GigaSMART Groups list.</p> <p>d. Enter gtp-flowsample-1 in the Alias field.</p> <p>e. Select Flow Sampling from the GigaSMART Operations (GSOP) list and then select the Flow Sampling-GTP option.</p> <p>f. Select Load Balancing from the GigaSMART Operations (GSOP) list.</p> <p>g. Configure Load Balancing as follows:</p> <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMSI</li> </ul> <p>h. Click Save.</p> |
| 12.  | Configure a second level map for GTP flow sampling, the first flow sampling map. This map has 12 rules.<br><br>Traffic flow is sampled based on the rules in this map. Accepted    | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Type GTP-Sample-1 in the Alias field</li> </ul>                                                                                                                                                                                                                                                                                                                                                                 |

| Task | Description                                                                                                                                                                                                                                   | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | packets are forwarded to a load balancing port group.                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype.</li> <li>■ Select the virtual port vport1 configured in Task 3 for the Source</li> <li>■ Select a port group PG-Sampl-1 for the Destination</li> <li>■ Select the GigaSMART Operation configured in Task for from the GSOP list</li> </ul> <p>d. Use the Add a Rule button to create the following flow sampling rules:</p> <ul style="list-style-type: none"> <li>■ Percentage 75, IMSI 3182609833*, IMEI 35609506*</li> <li>■ Percentage 10, IMSI 3182609834*, IMEI 3560950*</li> <li>■ Percentage 20, IMSI 31826098350*, IMEI 356095*</li> <li>■ Percentage 20, IMSI 31826098351*, IMEI 35609*</li> <li>■ Percentage 20, IMSI 31826098352*, IMEI 3560*</li> <li>■ Percentage 20, IMSI 31826098353*, IMEI 356*</li> <li>■ Percentage 20, IMSI 31826098354*, IMEI 35*</li> <li>■ Percentage 20, IMSI 31826098355*, IMEI 31*</li> <li>■ Percentage 20, IMSI 31826098356*, IMEI 356095*</li> <li>■ Percentage 20, IMSI 31826098356*, IMEI 356095*</li> <li>■ Percentage 20, IMSI 31826098357*, IMEI 3560*</li> <li>■ Percentage 20, IMSI 31826098358*, IMEI 35*</li> <li>■ Percentage 20, IMSI 31826098359*, IMEI 356095*</li> </ul> <p>e. Click Save.</p> |
| 13.  | <p>Configure a second level map for GTP flow sampling, the second flow sampling map. This map has 12 rules.</p> <p>Traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to a load balancing port group.</p> | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Type GTP-Sample-2 in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype.</li> <li>■ Select the virtual port vport1 configured in Task 2 for the Source</li> <li>■ Select a tool port group PG-Sample-2 for the Destination</li> <li>■ Select flow-sample-1 configured in Task 11 for from the GSOP list</li> </ul> <p>d. Use the Add a Rule button to create the following flow sampling rules:</p> <ul style="list-style-type: none"> <li>■ Percentage 30, IMSI 3182609836*, IMEI 35609506*</li> <li>■ Percentage 5, IMSI 3182609837*, IMEI 356095062*</li> <li>■ Percentage 50, IMSI 31826098380*, IMEI 356095062*</li> <li>■ Percentage 50, IMSI 31826098381*, IMEI 35609506*</li> </ul>                                                                                                                                                                                                                  |

| Task | Description                                                                                                                                                                                                                                   | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                               | <ul style="list-style-type: none"> <li>■ Percentage 50, IMSI 31826098382*, IMEI 3560950*</li> <li>■ Percentage 50, IMSI 31826098383*, IMEI 356095*</li> <li>■ Percentage 50, IMSI 31826098384*, IMEI 35*</li> <li>■ Percentage 50, IMSI 31826098385*, IMEI 356*</li> <li>■ Percentage 50, IMSI 31826098386*, IMEI 3560*</li> <li>■ Percentage 50, IMSI 31826098387*, IMEI 35609*</li> <li>■ Percentage 50, IMSI 31826098388*, IMEI 356095*</li> <li>■ Percentage 50, IMSI 31826098389*, IMEI 3560950*</li> </ul> <p>e. Click Save.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 14.  | <p>Configure a second level map for GTP flow sampling, the third flow sampling map. This map has 5 rules.</p> <p>Traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to a load balancing port group.</p>   | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>,</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Type GTP-Sample-3 in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype</li> <li>■ Select the virtual port vport1 configured in Task 3 for the Source</li> <li>■ Select a port group PG-Sample-3 port for the Destination</li> <li>■ Select flow-sample-1 configured in Task 11 for from the GSOP list</li> </ul> <p>d. Use the Add a Rule button to create the following flow sampling rules:</p> <ul style="list-style-type: none"> <li>■ Percentage 10, IMSI 31826098390*, IMEI 35609506*</li> <li>■ Percentage 10, IMSI 31826098391*, IMEI 35609506*</li> <li>■ Percentage 10, IMSI 31826098392*, IMEI 35609506*</li> <li>■ Percentage 10, IMSI 31826098393*, IMEI 35609506*</li> <li>■ Percentage 10, IMSI 31826098394*, IMEI 35609506*</li> </ul> <p>e. Click Save.</p> |
| 15.  | <p>Configure a second level map for GTP flow sampling, the fourth flow sampling map. This map has one rule.</p> <p>Traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to a load balancing port group.</p> | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Type GTP-Sample-4 in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype</li> <li>■ Select the virtual port vport1 configured in Task 3 for the Source</li> <li>■ Select a tool port for the Destination</li> <li>■ Select flow-sample-1 configured in Task 11 for from the</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Task | Description                                                              | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                          | <p>GSOP list</p> <p>d. Use the Add a Rule button to create the following flow sampling rule:</p> <ul style="list-style-type: none"> <li>■ Percentage 10, IMSI 31826098429*, IMEI 35609506*</li> </ul> <p>e. Click Save.</p>                                                                                                                                                                                                                                                                                                                       |
| 16.  | Configure a collector map for any packets that do not match other rules. | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Type GTP-Collector in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Collector for Subtype</li> <li>■ Select the virtual port vport1 configured in Task 3 for the Source</li> </ul> <p>d. Click Save.</p> |

## Example 6: APN for GTP Whitlelisting, GTP Flow Sampling

Example 7 specifies APN patterns for GTP whitelisting and GTP flow sampling.

In Example 7, traffic from network ports go to the two first level maps (gtp\_to\_v1\_c and gtp\_to\_v1\_u) and then to the virtual port (v1).

In the whitelist map, if there is a match to the APN pattern and if the IMSI is present in the whitelist (IMSI), packets are forwarded to a tool port.

If there is not a match to an IMSI in the whitelist, the traffic is flow sampled based on the APN pattern in the flow sampling map. Accepted packets are forwarded to the same tool port as specified in the whitelist map.

Any unmatched traffic goes to a shared collector that sends it to a different tool port.

| Task | Description                                                  | UI Steps                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure a network port and two tool ports and enable them. | <p>a. Go to <b>System &gt; Ports &gt; Ports &gt; All Ports</b>.</p> <p>b. Click Quick Port Editor.</p> <p>c. Configure a network port. Port 22/3/x3 in this example.</p> <p>d. Configure two tool ports. Port 22/4/x18 and 22/4/x19 in this</p> |

| Task | Description                                                                       | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                   | <p>example.</p> <ol style="list-style-type: none"> <li>Admin enable the ports by selecting Enable for each port.</li> <li>Click OK.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 2.   | Configure a GigaSMART group and associate it with two GigaSMART engine port.      | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>Click New.</li> <li>Type an gsg2 in the Alias field.</li> <li>In the Port List field, select the engine ports, which are 22/2/e1 and 22/2/e2 in this example</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 3.   | Create a virtual port.                                                            | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</li> <li>Type v1 in the Alias field.</li> <li>Select the GigaSMART Group created in Task 2 from the GigaSMART Group list.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 4.   | Configure two first level maps, one for control traffic and one for user traffic. | <ol style="list-style-type: none"> <li>Configure the first map as follows: <ul style="list-style-type: none"> <li>Alias: gtp_to_v1_c</li> <li>Type and subtype: First Level By Rule</li> <li>Source: 22/3/x3</li> <li>Destination: virtual port created in Task 2.</li> <li>Rule 1: Pass, Bi Directional, Port Destination 2123</li> <li>Rule 2: Pass, Bi Directional, Port Destination 2122</li> </ul> </li> <li>Save the map</li> <li>Configure the second map as follows: <ul style="list-style-type: none"> <li>Alias: gtp_to_v1_u</li> <li>Type and subtype: First Level By Rule</li> <li>Source: 22/3/x3.</li> <li>Destination: virtual port created in Task 2.</li> <li>Rule 1: Pass, Bi Directional, Port Destination 2152</li> <li>Rule 1: Pass, Bi Directional, IPv4 Fragmentation, Value: allFragNoFirst.</li> </ul> </li> <li>Save the map</li> </ol> |
| 5.   | Create the GTP whitelist.                                                         | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GTP Whitelist</b>.</li> <li>Click New.</li> <li>Enter gtp-whitelist in the Alias field</li> <li>Go to Task 6.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 6.   | Fetch whitelist files from a                                                      | <ol style="list-style-type: none"> <li>On the GTP Whitelist page, select Bulk Upload.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Task | Description                                                                                                                                                                                  | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | specified location to populate the GTP whitelist.                                                                                                                                            | <ol style="list-style-type: none"> <li>Select Bulk Entry Operation for IMSI Upload Type</li> <li>Select Upload from URL from the Bulk Upload Type list.</li> <li>Select Append.</li> <li>Enter the URL in the Enter Remote URL field. For example, <code>http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx</code></li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                  |
| 7.   | (Optional) Add a single IMSI to the GTP whitelist.                                                                                                                                           | <ol style="list-style-type: none"> <li>On the GTP Whitelist page, select Individual Entry Operation.</li> <li>Select Append for Operation Type</li> <li>Enter the IMSI entry in the Individual IMSI Entry field.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 8.   | Associate the GigaSMART group to the GTP whitelist.                                                                                                                                          | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</b></li> <li>Select GS Group gsg2 created in Task 2 and click Edit</li> <li>Under GTP Whitelist, click on the GTP Whitelist Alias field and select. gtp-whitelist</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                  |
| 9.   | Configure the GigaSMART operation for GTP whitelisting.                                                                                                                                      | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</b></li> <li>Click New.</li> <li>Select the GigaSMART Group gsg2 created in Task 2 and associated with the GTP whitelist in Step 8.</li> <li>Enter gtp-correlat_gsp_wl in the Alias field.</li> <li>Select GTP Whitelist from the GigaSMART Operations (GSOP) list</li> <li>Select Load Balancing from the GigaSMART Operations (GSOP) list.</li> <li>Configure Load Balancing as follows: <ol style="list-style-type: none"> <li>Select Stateful</li> <li>Set Type to GTP</li> <li>Select Hashing</li> <li>Select IMSI</li> </ol> </li> <li>Click Save.</li> </ol> |
| 10.  | Configure a second level map for GTP whitelisting, the whitelist map. If there is a match to the APN pattern and if IMSI is present in the whitelist (IMSI), it is forwarded to a tool port. | <ol style="list-style-type: none"> <li>On the left navigation pane, go to <b>Inventory  and from Traffic select Maps &gt; Maps &gt; Maps.</b></li> <li>Click New</li> <li>Configure the map. <ol style="list-style-type: none"> <li>Enter GTP-Whitelist in the Alias field.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                                                                                             |

| Task | Description                                                                                                                                                                                                                                                                                | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>■ Select Second Level for Type</li> <li>■ Select Flow Whitelist for Subtype</li> <li>■ Select gtp-correlate_gsg_wl from the GSOP list.</li> <li>■ Select the virtual port v1 configured in Task 3 for Source</li> <li>■ Select 22/4/x18 for Destination</li> <li>■ Rule 1: GTP, APN: mobile.com</li> </ul> <p>d. Click Save.</p>                                                                                                                                                                                                                                                                                                                                              |
| 11.  | Configure the GigaSMART operation for GTP flow sampling.                                                                                                                                                                                                                                   | <p>a. From the left navigation pane, go to <b>System &gt; GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation</b>.</p> <p>b. Click New.</p> <p>c. Select the GigaSMART Group gsg2 created in Task 2 and associated with the GTP whitelist in Step 8.</p> <p>d. Enter gtp-correlat_gsp_fs in the Alias field.</p> <p>e. Select GTP Whitelist from the GigaSMART Operations (GSOP) list</p> <p>f. Select Load Balancing from the GigaSMART Operations (GSOP) list.</p> <p>g. Configure Load Balancing as follows:</p> <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMSI</li> </ul> <p>h. Click Save</p>             |
| 12.  | Configure a second level map for GTP flow sampling, the flow sampling map. If there is not a match to an IMSI in the whitelist, the traffic flow is sampled based on the APN pattern in this map. Accepted packets are forwarded to the same tool port as specified in the whitelelist map | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>■ Type from_vp_fs1 in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Flow Sample for Subtype.</li> <li>■ Select the virtual port v1 configured in Task 3 for the Source</li> <li>■ Select a 22/4/x18 for the Destination</li> <li>■ Select the GigaSMART Operation gtp-correlate_gsg_fs</li> <li>■ Rule 1: GTP, Percentage: 100, APN: imsi*</li> </ul> <p>d. Click Save.</p> |
| 13.  | Add a shared collector for any unmatched traffic from the virtual port and send it to a different tool                                                                                                                                                                                     | <p>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Task | Description | UI Steps                                                                                                                                                                                                                                                                                                                                                                     |
|------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | port.       | <ol style="list-style-type: none"> <li>b. Click New.</li> <li>c. Configure the map. <ul style="list-style-type: none"> <li>■ Type from_vp_scroll in the Alias field</li> <li>■ Select Second Level for Type</li> <li>■ Select Collector for Subtype</li> <li>■ Select the virtual port v1 configured in Task 3 for the Source</li> </ul> </li> <li>d. Click Save.</li> </ol> |

## Example 7: APN for FTP Whitelisting, APN and QCI for GTP Flow Sampling

Example 6 specified APN patterns for GTP whitelisting and GTP flow sampling. It also specifies QCI for GTP flow sampling.

In Example 7, traffic from network ports go to the two first level maps (gtp\_to\_v1\_c and gtp\_to\_v1\_u) and then to the virtual port (v1).

In the whitelist map, if there is a match to the APN pattern and if the IMSI is present in the whitelist (IMSI), packets are forwarded to a tool port.

If there is not a match to an IMSI in the whitelist, the traffic is flow sampled based on the APN pattern and QCI value in the flow sampling map. Accepted packets are forwarded to the same tool port as specified in the whitelist map. Only 50% of traffic with QCI 5 is sent to the tool port.

Any unmatched traffic goes to a shared collector that sends it to a different tool port.

| Task | Description                                                  | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Configure a network port and two tool ports and enable them. | <ol style="list-style-type: none"> <li>a. Go to <b>System &gt; Ports &gt; Ports &gt; All Ports</b>.</li> <li>b. Click Quick Port Editor.</li> <li>c. Select a port (for example, 22/2/x3) and set Type to Network.</li> <li>d. Select a port (for example, 22/2/x18) and set Type to Tool</li> <li>e. Select a second port (for example, 22/2/x19) and set Type to Tool.</li> <li>f. Select Enable for Admin on the network and two tool ports.</li> <li>g. Click OK.</li> </ol> |

| Task | Description                                                                      | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2.   | Configure a GigaSMART group and associate it with two GigaSMART engine ports     | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Groups &gt; GigaSMART Groups</b>.</li> <li>Click New.</li> <li>Type gsg2 in the Alias field.</li> <li>Click in the Port List field and select two engine ports. For example, 22/2/e1 and 22/2/e2</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 3.   | Create a virtual port.                                                           | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;Virtual Ports</b>.</li> <li>Type v1 in the Alias field.</li> <li>Click in the GigaSMART Group field and select the GigaSMART Group created in Task 2.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 4.   | Configure two first level maps, one for control traffic and one for user traffic | <ol style="list-style-type: none"> <li>Configure the first map as follows: <ul style="list-style-type: none"> <li>Alias: gtp_to_v1_c</li> <li>Type and Subtype: First Level By Rule</li> <li>Enable Control Traffic.</li> <li>Source: 22/2/3/x3 (network port created in Task 1)</li> <li>Destination: v1 (virtual port created in Task 3)</li> <li>Rule 1: Pass, Bi Directional, Port Destination 2123</li> <li>Rule 2: Pass, Bi Directional, Port Destination 2122</li> </ul> </li> <li>Save the map</li> <li>Configure the second map as follows: <ul style="list-style-type: none"> <li>Alias: gtp_to_v1_u</li> <li>Type and subtype: First Level By Rule</li> <li>Source: 22/2/3/x3 (network port created in Task 1)</li> <li>Destination: v1 (virtual port created in Task 3)</li> <li>Rule 1: Pass, Bi Directional, Port Destination 2152</li> <li>Rule 2: Pass, Bi Directional, IPv4Fragmentation allFragNoFirst</li> </ul> </li> <li>Save the map</li> </ol> |
| 5.   | Associate the GigaSMART group to the active GTP Whitelist                        | <ol style="list-style-type: none"> <li>From the device view, select <b>GigaSMART &gt; GigaSMART Groups</b>.</li> <li>Select the GigaSMART Group created in Task 1 and click Edit.</li> <li>Locate the GTP Whitelist param, and enter the alias of whitelist in the GTP Whitelist Alias field. For example, IMSI.</li> <li>Save the GigaSMART Group.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Task | Description                                                                                                                                                                                            | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6.   | Configure the GigaSMART operation for GTP whitelisting.                                                                                                                                                | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</b></li> <li>Click New.</li> <li>Select the GigaSMART Group gsg1 created in Task 2 from the GigaSMART Groups list.</li> <li>Enter gtp-correlate_gsp_wl in the Alias field.</li> <li>Select GTP Whitelist from the GigaSMART Operations (GSOP) list</li> <li>Select Load Balancing from the GigaSMART Operations (GSOP) list.</li> <li>Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMSI</li> </ul> </li> <li>Click Save.</li> </ol> |
| 7.   | Configure a second level map for GTP whitelisting, the whitelist map. If there is a match to the APN pattern and if the IMSI is present in the whitelist (IMSI), packets are forwarded to a tool port. | <ol style="list-style-type: none"> <li>On the left navigation pane, go to <b>Inventory </b> and from <b>Traffic select Maps &gt; Maps &gt; Maps.</b></li> <li>Click New</li> <li>Configure the map. <ul style="list-style-type: none"> <li>■ Alias: GTP-whitelist</li> <li>■ Type an Subtype: Second Level Flow Whitelist</li> <li>■ Source: v1 (virtual port created in Task 3)</li> <li>■ Destination: 22/4/x18</li> <li>■ GSOP: gtp-corelate_gsg_wl</li> <li>■ Select gtp-whitelist from the GSOP list.</li> <li>■ Rule: GTP, APN: mobile.com</li> </ul> </li> <li>Click Save.</li> </ol>                                            |
| 8.   | Configure the GigaSMART operation for GTP flow sampling.                                                                                                                                               | <ol style="list-style-type: none"> <li>From the left navigation pane, go to <b>System &gt; GigaSMART &gt;GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</b></li> <li>Click New.</li> <li>Select the GigaSMART Group created in Task 2 from the GigaSMART Groups list.</li> <li>Enter gtp-corelate_gsg_fs in the Alias field.</li> <li>Select Flow Sampling from the GigaSMART Operations (GSOP) list and then select the Flow Sampling-GTP option.</li> <li>Select Load Balancing from the GigaSMART Operations (GSOP) list.</li> </ol>                                                                                                                                                                             |

| Task | Description                                                                                                                                                                                                                                                                               | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>g. Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>■ Select Stateful</li> <li>■ Set Type to GTP</li> <li>■ Select Hashing</li> <li>■ Select IMEI</li> </ul> </li> <li>h. Click Save.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 9.   | Configure a second level map for GTP flow sampling, the flow sampling map. If there is not a match to an IMSI in the whitelist, the traffic flow is sampled based on the APN pattern in this map. Accepted packets are forwarded to the same tool port as specified in the whitelist map. | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New.</li> <li>c. Configure the map. <ul style="list-style-type: none"> <li>■ Alias: from_vp_fs1</li> <li>■ Type and Subtype: Second Level Flow Sample</li> <li>■ Source: vp1</li> <li>■ Destination: 22/4/x18</li> <li>■ GSOP: gtp-corelate_gsg_fs</li> <li>■ Rule 1: GTP, APN: *imsi*, QCI: 5, Percentage: 50</li> <li>■ Rule 2: GTP, IMSI: ims*, Percentage 100</li> </ul> </li> <li>d. Click Save.</li> </ul> |
| 10.  | Add a shared collector for any unmatched traffic from the virtual port and send it to a different tool port.                                                                                                                                                                              | <ul style="list-style-type: none"> <li>a. On the left navigation pane, go to <b>Inventory</b>  and from <b>Traffic</b> select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click New.</li> <li>c. Configure the map: <ul style="list-style-type: none"> <li>■ Alias: from_vp_scoll</li> <li>■ Type and Subtype: Regular Collector</li> <li>■ Source: v1</li> <li>■ Destination: 22/4/x19</li> </ul> </li> <li>d. Click Save.</li> </ul>                                                                                                                                                          |

## 4G/5G Traffic Monitoring using UPN

In 4G/5G traffic monitoring using User Processing Node (UPN), the UPN processes the subscriber information that is extracted from the PFCP packets and correlates with the GTP-u traffic without the CPN. When the traffic contains the user's field information such as IMSI, IMEI, you can use the 4G/5G traffic monitoring using UPN.

The PFCP allows optional Informational Elements (IE) that contain SUPI/IMSI, PEI/IMEI, and GPSI/MSISDN information of the subscriber during PFCP session establishment request.

**NOTE:** The amount of time to restore from backup can take up to 11 minutes.

The UPN performs the following activities in the Standalone mode:

- Processes the PFCP session establishment request and extracts the SUPI/IMSI, PEI/IMEI, GPSI/MSISDN User IP, and TEID for both endpoints. The information in the PFCP traffic is used to populate the UPN's session table.
- Correlates GTP-U traffic based on the subscriber information from PFCP. The GTP-U look-up is correlated based on the IP and TEID.

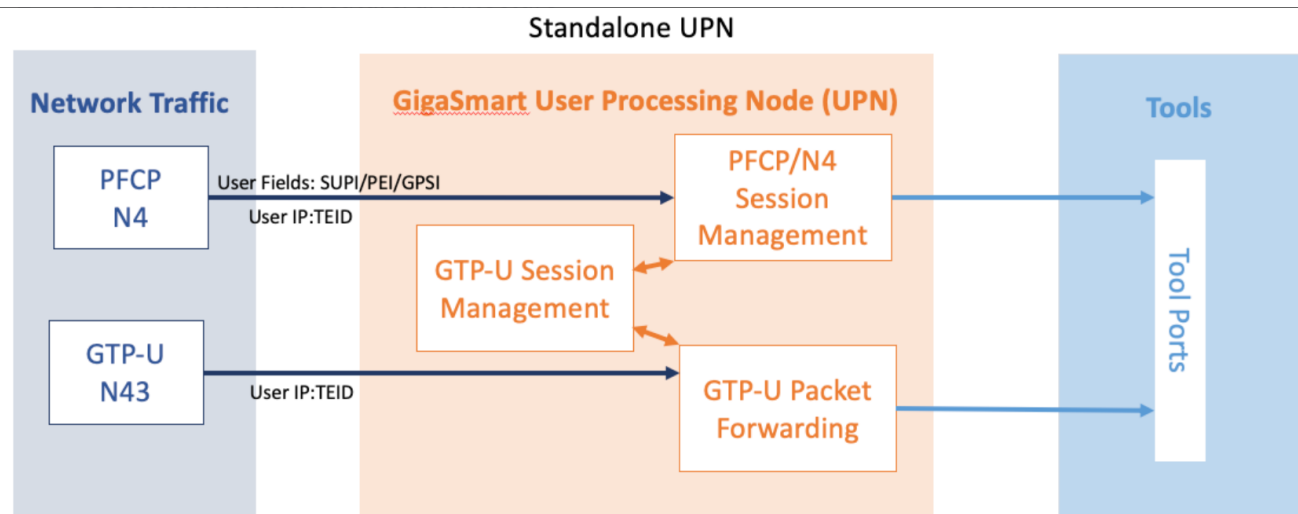
## What is PFCP?

PFCP (Packet Forwarding Control Protocol) is a 3GPP Protocol that is communicated on the Sx/N4 interface between the Control Plane (CP) elements and User Plane (UP) elements. The CP element programs the UP element with policies on how to forward packets. PFCP packets convey information in the form of Information Elements (IE). PFCP allows an optional IE called User Fields that contains IMSI/SUPI, IMEI/PEI, MSISDN/GPSI information of the Subscriber during PFCP Session Establishment Request.

The PFCP (Packet Forwarding Control Protocol) is a 3GPP Protocol that is communicated on Sxa, Sxb, N4 interface between the Control Plane (CP) elements and User Plane (UP) elements.

The CP element programs the UP element with policies on how to forward packets. The CP function controls packet processing in the UP function by establishing, modifying, and deleting the PFCP session.

The following diagrams explain the functioning of UPN in Stand-alone mode:



## Rules and Notes

- A Stand-alone UPN traffic monitoring session can be created only when there is atleast SUPI in the user fields.
- You cannot perform RAN correlation or Network Slicing Correlation in Stand alone UPN traffic monitoring
- UPN does not receive SFFP messages in the User field parse mode.

### Configure 4G/5G Traffic Monitoring using UPN

The following are the points to remember while configuring 4G/5G traffic monitoring using UPN:

- You must enable the stand-alone mode in UPN while creating the solution in Ansible.
- Once the stand-alone mode is enabled, UPN cannot connect with the CPN, and you cannot change the mode. To change the mode, you need to delete the UPN from the solution and
- add a new one.

## PFCP Messages

### Session Related Messages

These messages are exchanged between Control Plane and User Plane function at the subscriber level. These messages are load balanced based on the **IMSI** of the subscriber.

- Session establishment request/response
- Session modification request/response
- Session deletion request/response
- Session report request/response

### Node Related Messages

The PFCP node related message packets are broadcast to all the ports which are part of the port-group in FS/WL maps. These messages are not specific to any subscriber. The load balancing based on **IMSI** is not possible for these packets. They continue to broadcast as per the existing behavior.

- Heartbeat request/response
- PFCP PFD management request/response
- PFCP association setup request/response
- PFCP association update request/response
- PFCP association release request/response
- Version Not supported response
- PFCP Node report request/response
- PFCP session set deletion request/response

### PFCP Load Balancing

The PFCP packets received are load balanced based on the **IMSI** present in the "IE Type: UserID".

Once the PFCP packet is received, the mobility application will parse the packet and create or update or delete the corresponding sessions or tunnels in the session table. The IMSI present in "IE Type: UserId" is stored in the session table and used for load balancing. Once sessions or tunnels are created, map lookup is performed for the PFCP packets. If there is a match in the IMSI, the packet is sent to only one port from the configured **Load Balancing** application based on the **IMSI** hashing. The hash value string from IMSI string present in the "IE Type: UserId" is added to the packet before sending to the **Load Balancing** application. The **Load Balancing** application will do **Load Balancing** logic based on this hash string and choose any one port to send the packet out.

**Licensing Requirement:** There is no need of a separate license for PFCP Load balancing. The existing license for Standalone UPN is sufficient for this feature.

**Single Engine:** The PFCP packet is sent to only one GigaSMARTS engine. Based on the map lookup, the packet will be forwarded to the **Load Balancing** application and sent to only one port based on the IMSI hashing.

**Grouped Engine:** The PFCP packet is sent to all the GigaSMART engines configured as part of the engine group configuration. The PFCP packets are processed as per the existing design, but the packets are sent out only through one port in the **LoadBalancing** application in the leader engine.

### Map Configuration

The 4G and 5G traffic passes through a single map in standalone mode. The user can configure a 4G map through which both 4G and 5G traffic passes. You do not need to configure separate maps for 4G and 5G traffic.

**NOTE:** The single map configuration is applicable only for standalone UPN. For legacy GTP and 5G user need to configure 4G and 5G maps separately

### Required License for UPN Standalone Single Map type: 5G.

- For 5G and GTP flow sample with rule percentage (0 or 100), the **5GC** and **GTP\_MAX** licenses are required.
- For 5G and GTP flow sample with rule percentage in all ranges (between 0 to 100) or for GTP Whitelist, the **5GC**, **GTP\_MAX**, and **FVUE** licenses are required.

### Stateful Session Recovery

It is crucial to back up the information from the correlated session table to avoid discrepancies during engine reboots and connection failures. After a successful reboot, the information saved as part of the persistence file is populated back into the mobility database.

Mobility applications require stateful session recovery to persist their data between node reboots and connection failures. This feature aims to extend the support available in LTE/5G mobility applications to Standalone UPN functionality. The session table is backed up every 10 minutes. You cannot change the backup time interval.

**File Age Timeout**— Specifies the time the backup file is valid, in minutes. After this time expires, the backup file is stale. The default is 30 minutes.

<10 ~ 1440> - 10 minutes is the minimum and 1440 minutes is the maximum value for file-age-timeout.

**Restart Age Timeout**—Specifies the time interval following a reboot for aging-out sessions, in minutes. This is a shorter interval than that specified using the gtp-flow timeout. The gtp-flow timeout disconnects a GTP session if it has been inactive for the timeout value, which has a default of 8 hours. The restart-age-timeout default is 30 minutes.

<10 ~ 1440> - 10 minutes is the minimum and 1440 minutes is the maximum value for restart-age-timeout

**GTP Persistence Interval**—Specifies the time interval between backups, in minutes. The default is 10 minutes.

<10 ~ 1440> - 10 minutes is the minimum and 1440 minutes is the maximum value for restart-age-timeout.

| GTP Persistence                            |                                     |
|--------------------------------------------|-------------------------------------|
| GTP Persistence                            | <input checked="" type="checkbox"/> |
| GTP Persistence Interval (minutes)         | 10                                  |
| GTP Persistence Restart Age Time (minutes) | 20                                  |
| GTP Persistence File Age Timeout (minutes) | 30                                  |
| GTP Backup Files                           | <button>Delete All</button>         |

## 5G Stateful Session Recovery

Required License: 5G Correlation

5G stateful session recovery provides session persistence for GigaSMART 5G applications, including 5G flow filtering, 5G forward listing, and 5G flow sampling. In this method of recovery, 5G sessions are backed up periodically so that they can be recovered faster after a GigaSMART line card reboot or a node reboot.

5G stateful session recovery requires additional memory for storing backups. GigaVUE-HC3 has the required memory.

Using 5G stateful session recovery, the 5G session tables in the GigaSMART line card memory are periodically backed up to the control card memory on the node and stored.

You should configure an interval for how often the backups occur, such as every 10 minutes. If 5G stateful session recovery is enabled and the GigaSMART line card is rebooted, the 5G session tables are restored automatically following the reboot.

The last stored backup file is downloaded from the control card to the GigaSMART line card using FTP. The session table is repopulated from the last stored backup file to each GigaSMART engine, up to 8 engines. Packet count statistics for sessions are saved and restored.

Depending on the size of the session table, the amount of time to restore from the backup might take as much as 3 minutes. During that interval, traffic is blocked to the virtual port on the GigaSMART line card. Once the session table is read and populated, traffic is allowed.

Depending on the interval between backups, there could be differences between the stored state and the current state of the system, for example, map configuration could change, or sessions could be added, modified, or deleted.

Load balancing information is not persisted, so after a session table is repopulated, a session that was once sent to one load-balanced port may be sent to a different load-balanced port after the reboot. However, for SUPI-based load balancing, the traffic is sent to the same port as it was before the reboot.

5G stateful session recovery works in a cluster environment; however, the cluster leader must remain the same.

### Configure 5G Stateful Session Recovery

To enable 5G stateful session recovery, as well as to configure timers, do the following:

1. On the left navigation pane, click , and then select **Physical>Nodes**.
2. From the device view, select **GigaSMART > GigaSMART groups**.
3. Click on the alias of the **GigaSMART group**.
4. Select **GTP Persistence** in the **GTP Persistence** fields under GigaSMART Parameters. The timers are pre-configured with default values.



The screenshot shows a configuration page for 'GTP Persistence'. At the top, there is a header 'GTP Persistence' with a dropdown arrow. Below it, there is a table with four rows of configuration parameters. Each row has a label, a value, and a reset icon. The first row is 'GTP Persistence' with a checked checkbox. The second row is 'GTP Persistence Interval (minutes)' with a value of 10. The third row is 'GTP Persistence Restart Age Time (minutes)' with a value of 30. The fourth row is 'GTP Persistence File Age Timeout (minutes)' with a value of 30.

| GTP Persistence                            |                                     |  |
|--------------------------------------------|-------------------------------------|--|
| GTP Persistence                            | <input checked="" type="checkbox"/> |  |
| GTP Persistence Interval (minutes)         | 10                                  |  |
| GTP Persistence Restart Age Time (minutes) | 30                                  |  |
| GTP Persistence File Age Timeout (minutes) | 30                                  |  |

**Figure 18** *GTP Persistence GigaSMART Parameters*

Use the **System** widget on the Overview page to determine the amount of memory. The size of memory is 24Gb in an upgraded system.

## **View Backup and Restore Information**

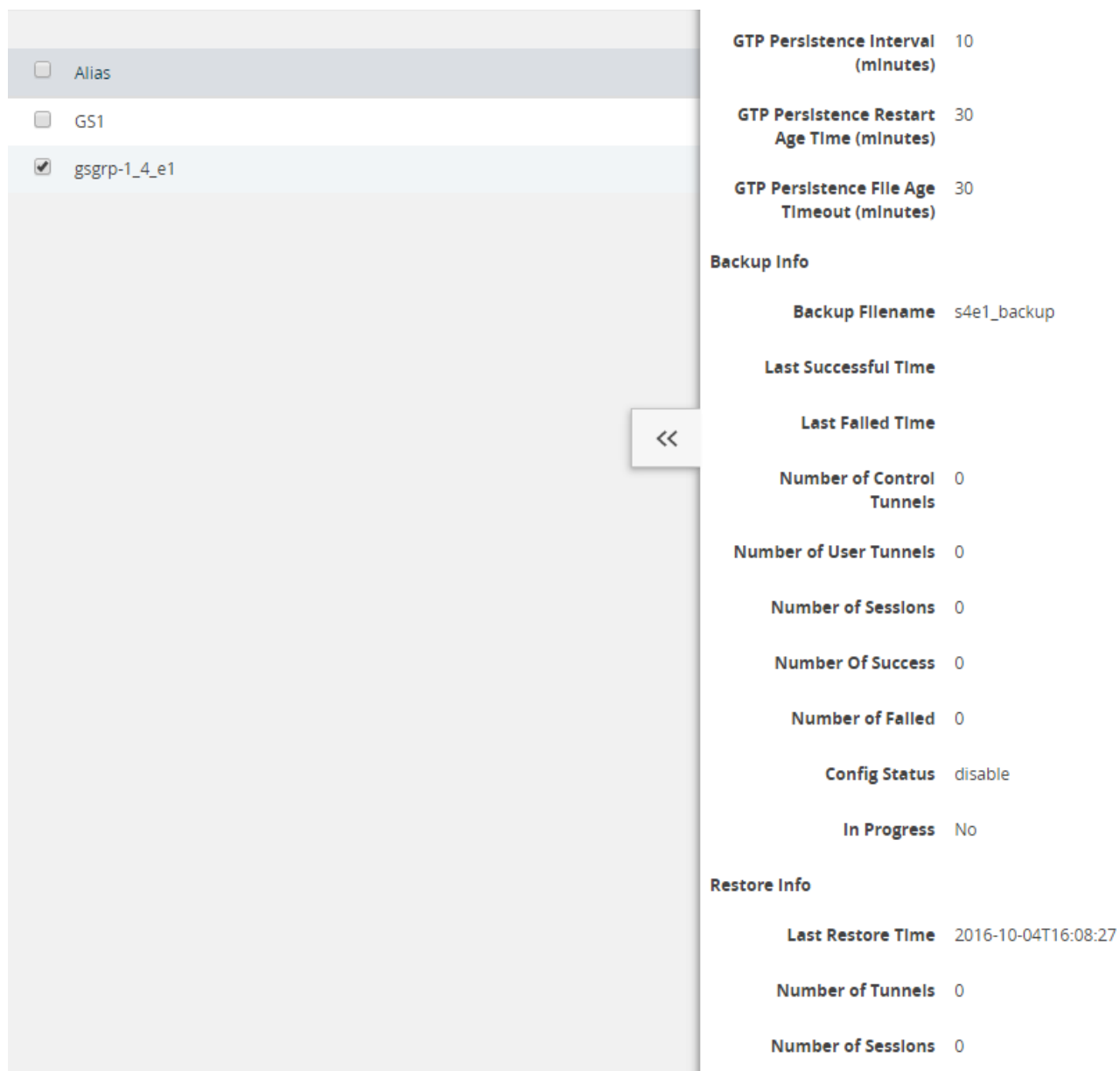
To view the System information, select **Overview** from the Navigation pane. The amount of free and used memory is displayed in the **Memory** field.

To view backup and restore information for GTP Persistence:

1. Select **GigaSMART > GigaSMART Groups > GigaSMART Group**.
2. Click on the alias of the GigaSMART group.

A Quick View appears for the selected GigaSMART group.

3. Scroll down to GTP Persistence. In Figure 26-63, GigaSMART Group gsggrp-1\_4\_e1 is selected and the Quick View is displayed.



The screenshot displays the configuration interface for GTP Persistence Information. On the left, a list of profiles is shown with checkboxes: 'Alias' (unchecked), 'GS1' (unchecked), and 'gsgpr-1\_4\_e1' (checked). A double-left arrow button is visible next to the 'gsgpr-1\_4\_e1' profile. The right side of the interface shows the configuration details for the selected profile.

|                                                   |                     |
|---------------------------------------------------|---------------------|
| <b>GTP Persistence Interval (minutes)</b>         | 10                  |
| <b>GTP Persistence Restart Age Time (minutes)</b> | 30                  |
| <b>GTP Persistence File Age Timeout (minutes)</b> | 30                  |
| <b>Backup Info</b>                                |                     |
| <b>Backup Filename</b>                            | s4e1_backup         |
| <b>Last Successful Time</b>                       |                     |
| <b>Last Failed Time</b>                           |                     |
| <b>Number of Control Tunnels</b>                  | 0                   |
| <b>Number of User Tunnels</b>                     | 0                   |
| <b>Number of Sessions</b>                         | 0                   |
| <b>Number Of Success</b>                          | 0                   |
| <b>Number of Failed</b>                           | 0                   |
| <b>Config Status</b>                              | disable             |
| <b>In Progress</b>                                | No                  |
| <b>Restore Info</b>                               |                     |
| <b>Last Restore Time</b>                          | 2016-10-04T16:08:27 |
| <b>Number of Tunnels</b>                          | 0                   |
| <b>Number of Sessions</b>                         | 0                   |

Figure 2 GTP Persistence Information

### Configure GTP Overlap Mapping

The configuration of GTP forward listing and GTP flow sampling maps that are part of the GTP overlap flow sampling map group follow the same configuration considerations discussed previously in GigaSMART GTP forward listing and GTP Flow Sampling. As is the case with regular non-overlap GTP mapping, GTP forward listing selects specific subscribers based on IMSI, whereas GTP flow sampling uses map rules to select subscribers and then forward a percentage of the packets to tool ports.

## Configuration Considerations

This section details certain configuration considerations that apply only to the configuration of GTP forward listing and flow sampling maps for GTP overlap flow sampling maps.

### About Standalone UPN Flow Sampling Map Mode and Port Groups

A second level type map specifying Standalone UPN flow sampling map mode must be selected to configure Standalone UPN forward listing and flow sampling maps.

To configure a Standalone UPN whitelisting map in overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Whitelist Overlap** in a map.

To configure a GTP flow sampling map in GTP overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Sample Overlap** in a map .

You can configure one GTP forward listing map and one GTP flow sampling map pair that contain traffic policies corresponding to one destination port group. The load balanced port groups can contain a single port, a port range, or a GigaStream. Note that, starting in software version 4.8, port groups used in GTP overlapping maps support GigaStream.

The maximum number of port groups per single GTP overlap flow sampling map group is six.

For more information about port groups, refer to Port Groups.

## Maximum Number of Port Group Members

The Maximum number of port group members can be determined as follows:

### Standalone Configuration

In a standalone configuration, use the following sequence :

1. Determine the number of members per port group and add 1.
2. Multiply each port group result by each other.
3. The total multiplication should not exceed 4096.

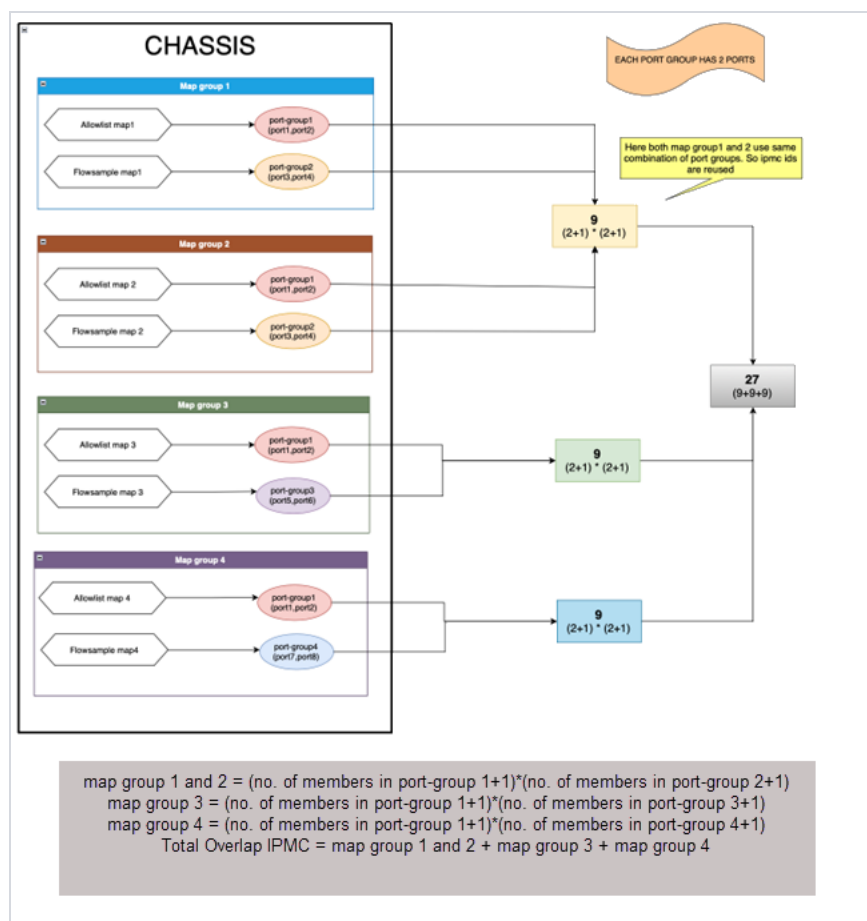
For instance, assume the following configuration in a GTP overlap mapping group:

- o Port Group 1–2 load-balanced GigaStream

- o Port Group 2–3 load-balanced GigaStream
- o Port Group 3–1 load-balanced tool port
- o Port Group 4–1 load-balanced GigaStream
- o Port Group 5–4 load-balanced tool ports. The total number becomes:  $(2+1) \times (3+1) \times (1+1) \times (1+1) \times (4+1) = 240$

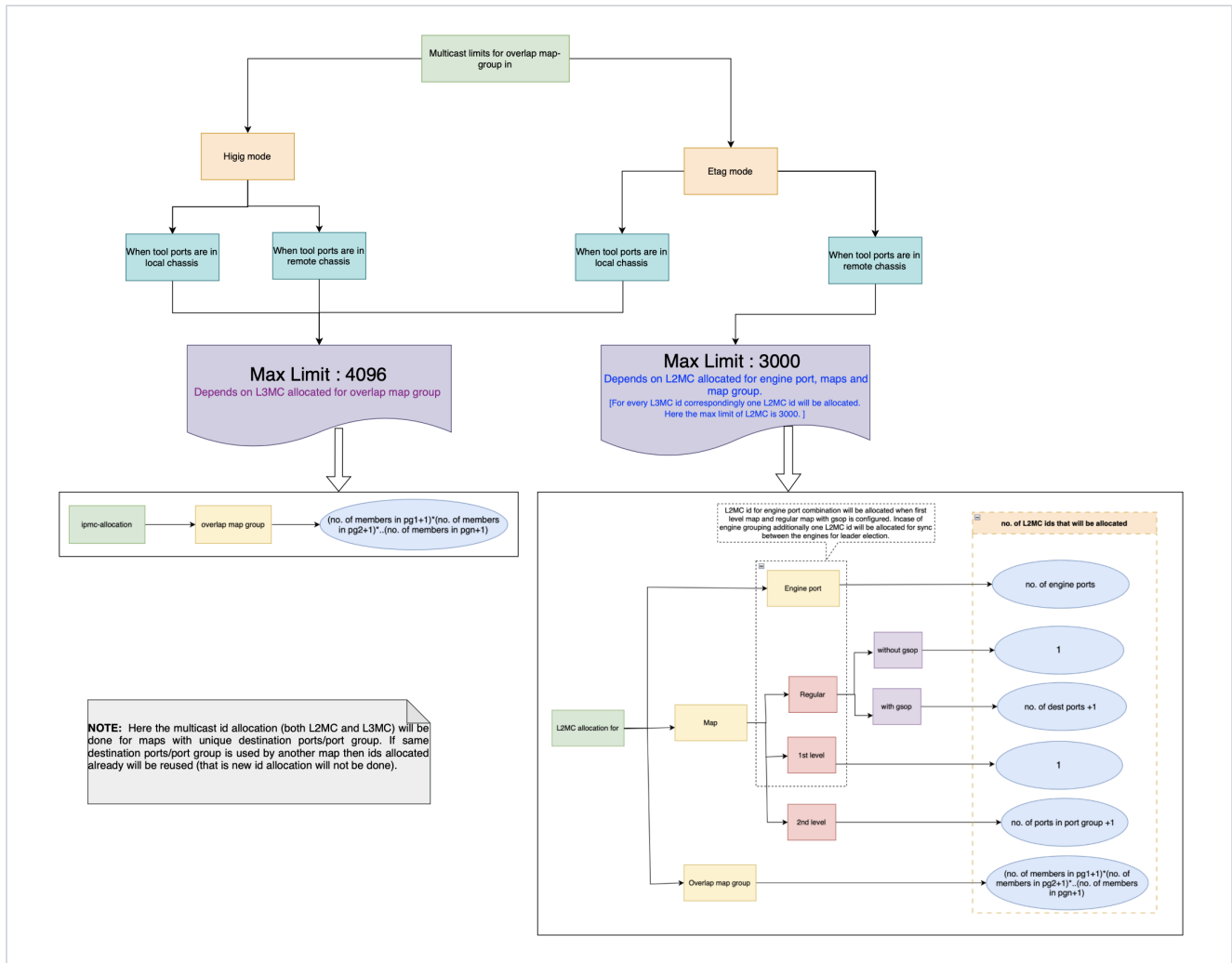
The tool configuration shown is accepted since this does not exceed the maximum number of multicast IDs (4096).

If Port Groups are utilized across multiple map groups in a single cluster, refer to the representation below on how the multicast IDs are calculated.



## Cluster Configuration

In a cluster configuration, Multicast IDs can defer based on Hi-Gig mode or E-tag mode. The below is representation of the same.



## Standalone UPN Flow Sampling Map Priority

Since a packet matches multiple maps independently the concept of second level map priority does not apply to Standalone UPN flow sampling maps. A standalone UPN flow sampling map pair consists of one Standalone UPN forward listing map and one Standalone UPN flow sampling map having the same destination port group. Within a Standalone UPN flow sampling map pair the forward listing map rules will be applied before the flow sampling map rules.

## Virtual Port Configuration in Standalone UPN Mode

In Standalone UPN map configuration, the virtual port sending traffic to all the port groups need to be configured in Standalone UPN mode.

To configure the virtual port with Standalone UPN mode, select Standalone UPN when configuring the virtual port.

### Overlap Support

Currently, a GTP packet can be destined to at most one destination tool. You can now receive multiple copies of a GTP packet that are sent to various tools (One copy per tool set).

## Standalone UPN

In Standalone User Plane Node (UPN) traffic monitoring, the UPN processes the subscriber information that is extracted from the Packet Forwarding Control Protocol (PFCP) packets and correlates with the GTP-U traffic without the CPN. The PFCP allows optional Informational Elements (IE) that contain SUPI/IMSI, PEI/IMEI, and GPSI/MSISDN information of the subscriber during PFCP session establishment request.

**NOTE:** The amount of time to restore from backup can take up to 11 minutes.

The UPN performs the following activities in the Standalone mode:

- Processes the PFCP session establishment request and extracts the SUPI/IMSI, PEI/IMEI, GPSI/MSISDN User IP, and TEID for both endpoints. The information in the PFCP traffic is used to populate the UPN's session table.
- Correlates GTP-U traffic based on the subscriber information from PFCP. The GTP-U look-up is correlated based on the IP and TEID.

### PFCP (Packet Forwarding Control Protocol)

The PFCP (Packet Forwarding Control Protocol) is a 3GPP Protocol that is communicated on Sxa, Sxb, N4 interface between the Control Plane (CP) elements and User Plane (UP) elements.

The CP element programs the UP element with policies on how to forward packets. The CP function controls packet processing in the UP function by establishing, modifying, and deleting the PFCP session.

## PFCP Messages

### Session Related Messages

These messages are exchanged between Control Plane and User Plane function at the subscriber level. These messages are load balanced based on the **IMSI** of the subscriber.

- Session establishment request/response
- Session modification request/response
- Session deletion request/response

- Session report request/response

## Node Related Messages

The PFCP node related message packets are broadcast to all the ports which are part of the port-group in FS/WL maps. These messages are not specific to any subscriber. The load balancing based on **IMSI** is not possible for these packets. They continue to broadcast as per the existing behavior.

- Heartbeat request/response
- PFCP PFD management request/response
- PFCP association setup request/response
- PFCP association update request/response
- PFCP association release request/response
- Version Not supported response
- PFCP Node report request/response
- PFCP session set deletion request/response

## PFCP Load Balancing

The PFCP packets received are load balanced based on the **IMSI** present in the "IE Type: UserID".

Once the PFCP packet is received, the mobility application will parse the packet and create or update or delete the corresponding sessions or tunnels in the session table. The IMSI present in "IE Type: UserID" is stored in the session table and used for load balancing. Once sessions or tunnels are created, map lookup is performed for the PFCP packets. If there is a match in the IMSI, the packet is sent to only one port from the configured **Load Balancing** application based on the **IMSI** hashing. The hash value string from IMSI string present in the "IE Type: UserID" is added to the packet before sending to the **Load Balancing** application. The **Load Balancing** application will do **Load Balancing** logic based on this hash string and choose any one port to send the packet out.

**Licensing Requirement:** There is no need of a separate license for PFCP Load Balancing. The existing license for Standalone UPN is sufficient for this feature.

**Single Engine:** The PFCP packet is sent to only one GigaSMARTS engine. Based on the map lookup, the packet will be forwarded to the **Load Balancing** application and sent to only one port based on the IMSI hashing.

**Grouped Engine:** The PFCP packet is sent to all the GigaSMART engines configured as part of the engine group configuration. The PFCP packets are processed as per the existing design, but the packets are sent out only through one port in the **Load Balancing** application in the leader engine.

## Map Configuration

The 4G and 5G traffic passes through a single map in standalone mode. The user can configure a 4G map through which both 4G and 5G traffic passes. You do not need to configure separate maps for 4G and 5G traffic.

**NOTE:** The single map configuration is applicable only for standalone UPN. For legacy GTP and 5G user need to configure 4G and 5G maps separately

Required License for UPN Standalone Single Map type: 4G and 5G.

### Stateful Session Recovery

It is crucial to back up the information from the correlated session table to avoid discrepancies during engine reboots and connection failures. After a successful reboot, the information saved as part of the persistence file is populated back into the mobility database.

Mobility applications require stateful session recovery to persist their data between node reboots and connection failures. This feature aims to extend the support available in LTE/5G mobility applications to Standalone UPN functionality. The session table is backed up every 10 minutes. You cannot change the backup time interval.

**File Age Timeout**— Specifies the time the backup file is valid, in minutes. After this time expires, the backup file is stale. The default is 30 minutes.

<10 ~ 1440> - 10 minutes is the minimum and 1440 minutes is the maximum value for file-age-timeout.

**Restart Age Timeout**—Specifies the time interval following a reboot for aging-out sessions, in minutes. This is a shorter interval than that specified using the gtp-flow timeout. The gtp-flow timeout disconnects a GTP session if it has been inactive for the timeout value, which has a default of 8 hours. The restart-age-timeout default is 30 minutes.

<10 ~ 1440> - 10 minutes is the minimum and 1440 minutes is the maximum value for restart-age-timeout

**GTP Persistence Interval**—Specifies the time interval between backups, in minutes. The default is 10 minutes.

<10 ~ 1440> - 10 minutes is the minimum and 1440 minutes is the maximum value for restart-age-timeout.

The screenshot shows a configuration panel titled "GTP Persistence". It contains the following settings:

- GTP Persistence:** A checkbox that is checked.
- GTP Persistence Interval (minutes):** A text input field with the value "10".
- GTP Persistence Restart Age Time (minutes):** A text input field with the value "20".
- GTP Persistence File Age Timeout (minutes):** A text input field with the value "30".
- GTP Backup Files:** A button labeled "Delete All".

## 5G Stateful Session Recovery

Required License: 5G Correlation

5G stateful session recovery provides session persistence for GigaSMART 5G applications, including 5G flow filtering, 5G forward listing, and 5G flow sampling. In this method of recovery, 5G sessions are backed up periodically so that they can be recovered faster after a GigaSMART line card reboot or a node reboot.

5G stateful session recovery requires additional memory for storing backups. GigaVUE-HC3 has the required memory.

Using 5G stateful session recovery, the 5G session tables in the GigaSMART line card memory are periodically backed up to the control card memory on the node and stored.

You should configure an interval for how often the backups occur, such as every 10 minutes. If 5G stateful session recovery is enabled and the GigaSMART line card is rebooted, the 5G session tables are restored automatically following the reboot.

The last stored backup file is downloaded from the control card to the GigaSMART line card using FTP. The session table is repopulated from the last stored backup file to each GigaSMART engine, up to 8 engines. Packet count statistics for sessions are saved and restored.

Depending on the size of the session table, the amount of time to restore from the backup might take as much as 3 minutes. During that interval, traffic is blocked to the virtual port on the GigaSMART line card. Once the session table is read and populated, traffic is allowed.

Depending on the interval between backups, there could be differences between the stored state and the current state of the system, for example, map configuration could change, or sessions could be added, modified, or deleted.

Load Balancing information is not persisted, so after a session table is repopulated, a session that was once sent to one Load Balanced port may be sent to a different Load Balanced port after the reboot. However, for SUPI-based Load Balancing, the traffic is sent to the same port as it was before the reboot.

5G stateful session recovery works in a cluster environment; however, the cluster leader must remain the same.

### Configure 5G Stateful Session Recovery

To enable 5G stateful session recovery, as well as to configure timers, do the following:

1. On the left navigation pane, click , and then select **Physical>Nodes**.
2. From the device view, select **GigaSMART > GigaSMART groups**.
3. Click on the alias of the **GigaSMART group**.

4. Select **GTP Persistence** in the **GTP Persistence** fields under GigaSMART Parameters. The timers are pre-configured with default values.

▼ GTP Persistence

GTP Persistence

☒

GTP Persistence Interval (minutes)

10

▲ ▼

GTP Persistence Restart Age Time (minutes)

30

▲ ▼

GTP Persistence File Age Timeout (minutes)

30

▲ ▼

**Figure 19**    *GTP Persistence GigaSMART Parameters*

Use the **System** widget on the Overview page to determine the amount of memory. The size of memory is 24Gb in an upgraded system.

**View Backup and Restore Information**

To view the System information, select **Overview** from the Navigation pane. The amount of free and used memory is displayed in the **Memory** field.

To view backup and restore information for GTP Persistence:

- 1. Select **GigaSMART > GigaSMART Groups > GigaSMART Group**.
- 2. Click on the alias of the GigaSMART group.

A Quick View appears for the selected GigaSMART group.

- 3. Scroll down to GTP Persistence. In Figure 26-63, GigaSMART Group gsgrp-1\_4\_e1 is selected and the Quick View is displayed.

The screenshot displays the configuration interface for GTP Persistence Information. On the left, a list of profiles is shown with checkboxes: 'Alias' (unchecked), 'GS1' (unchecked), and 'gsgpr-1\_4\_e1' (checked). A double-left arrow button is visible next to the 'gsgpr-1\_4\_e1' profile. The right side of the interface shows the configuration details for the selected profile.

|                                                   |                     |
|---------------------------------------------------|---------------------|
| <b>GTP Persistence Interval (minutes)</b>         | 10                  |
| <b>GTP Persistence Restart Age Time (minutes)</b> | 30                  |
| <b>GTP Persistence File Age Timeout (minutes)</b> | 30                  |
| <b>Backup Info</b>                                |                     |
| <b>Backup Filename</b>                            | s4e1_backup         |
| <b>Last Successful Time</b>                       |                     |
| <b>Last Failed Time</b>                           |                     |
| <b>Number of Control Tunnels</b>                  | 0                   |
| <b>Number of User Tunnels</b>                     | 0                   |
| <b>Number of Sessions</b>                         | 0                   |
| <b>Number Of Success</b>                          | 0                   |
| <b>Number of Failed</b>                           | 0                   |
| <b>Config Status</b>                              | disable             |
| <b>In Progress</b>                                | No                  |
| <b>Restore Info</b>                               |                     |
| <b>Last Restore Time</b>                          | 2016-10-04T16:08:27 |
| <b>Number of Tunnels</b>                          | 0                   |
| <b>Number of Sessions</b>                         | 0                   |

Figure 2 GTP Persistence Information

### Configure GTP Overlap Mapping

The configuration of GTP forward listing and GTP flow sampling maps that are part of the GTP overlap flow sampling map group follow the same configuration considerations discussed previously in GigaSMART GTP forward listing and GTP Flow Sampling. As is the case with regular non-overlap GTP mapping, GTP forward listing selects specific subscribers based on IMSI, whereas GTP flow sampling uses map rules to select subscribers and then forward a percentage of the packets to tool ports.

## Configuration Considerations

This section details certain configuration considerations that apply only to the configuration of GTP forward listing and flow sampling maps for GTP overlap flow sampling maps.

### About Standalone UPN Flow Sampling Map Mode and Port Groups

A second level type map specifying Standalone UPN flow sampling map mode must be selected to configure Standalone UPN forward listing and flow sampling maps.

To configure a Standalone UPN whilelisting map in overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Whitelist Overlap** in a map.

To configure a GTP flow sampling map in GTP overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Sample Overlap** in a map .

You can configure one GTP forward listing map and one GTP flow sampling map pair that contain traffic policies corresponding to one destination port group. The load balanced port groups can contain a single port, a port range, or a GigaStream. Note that, starting in software version 4.8, port groups used in GTP overlapping maps support GigaStream.

The maximum number of port groups per single GTP overlap flow sampling map group is six.

For more information about port groups, refer to Port Groups.

### Maximum Number of Port Group Members

The Maximum number of port group members can be determined as follows:

#### Standalone Configuration

In a standalone configuration, use the following sequence :

1. Determine the number of members per port group and add 1.
2. Multiply each port group result by each other.
3. The total multiplication should not exceed 4096.

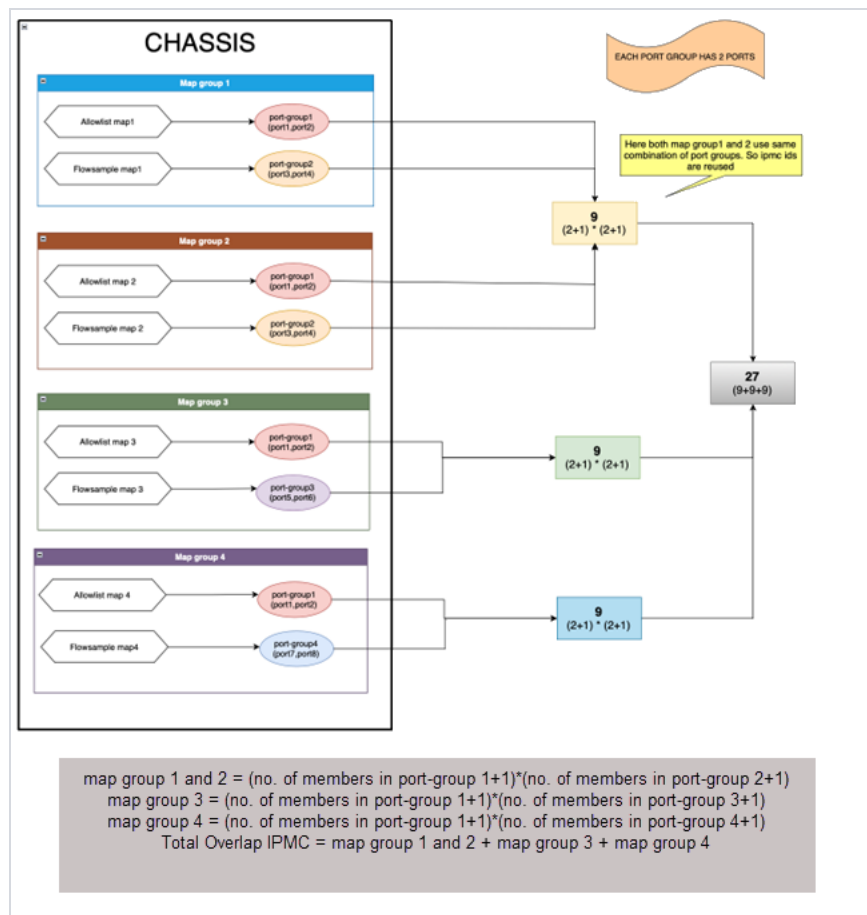
For instance, assume the following configuration in a GTP overlap mapping group:

- o Port Group 1–2 load-balanced GigaStream
- o Port Group 2–3 load-balanced GigaStream

- o Port Group 3—1 load-balanced tool port
- o Port Group 4—1 load-balanced GigaStream
- o Port Group 5—4 load-balanced tool ports. The total number becomes:  $(2+1)*(3+1)*(1+1)*(1+1)*(4+1) = 240$

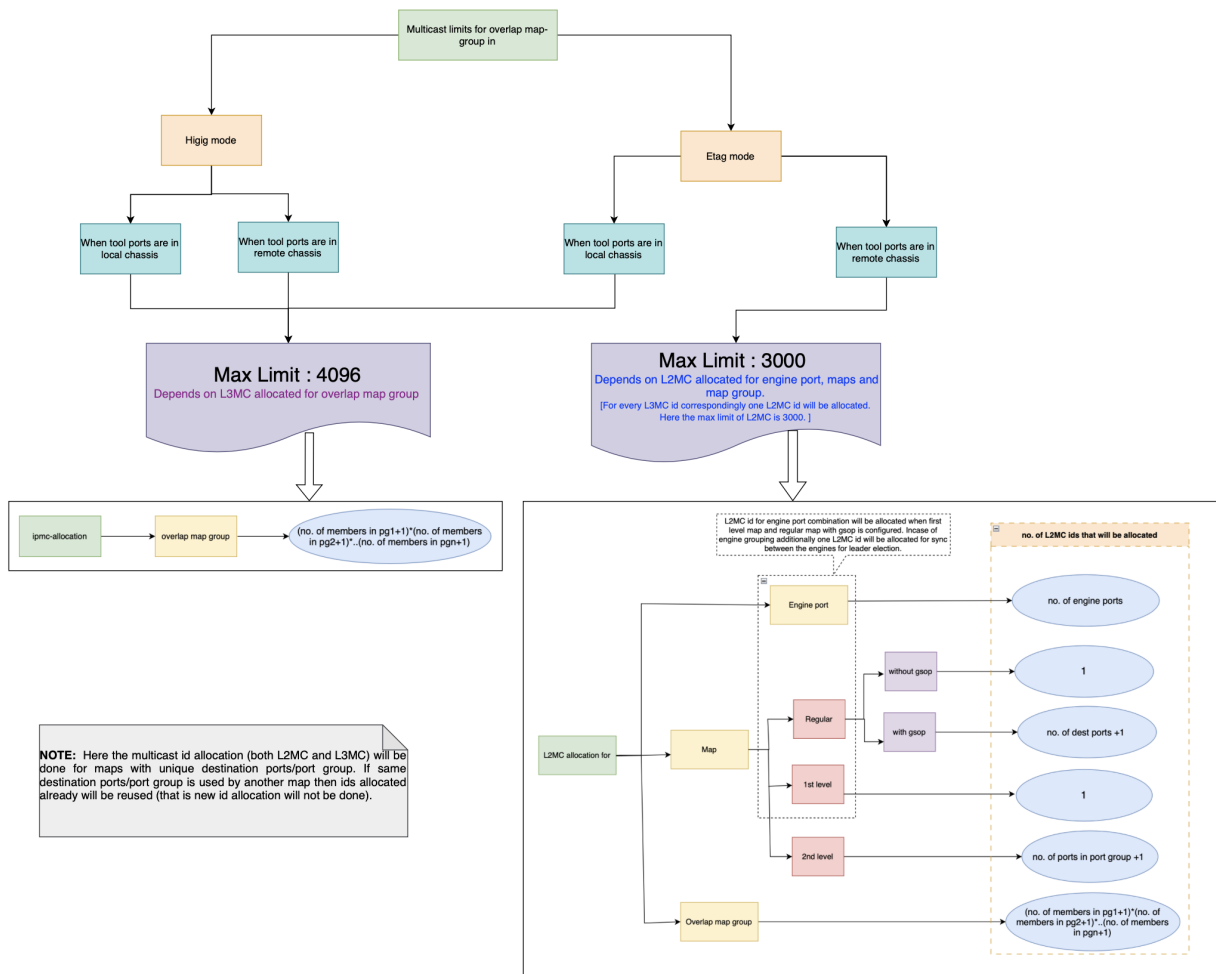
The tool configuration shown is accepted since this does not exceed the maximum number of multicast IDs (4096).

If Port Groups are utilized across multiple map groups in a single cluster, refer to the representation below on how the multicast IDs are calculated.



## Cluster Configuration

In a cluster configuration, Multicast IDs can defer based on Hi-Gig mode or E-tag mode. The below is representation of the same.



## Standalone UPN Flow Sampling Map Priority

Since a packet matches multiple maps independently the concept of second level map priority does not apply to Standalone UPN flow sampling maps. A standalone UPN flow sampling map pair consists of one Standalone UPN forward listing map and one Standalone UPN flow sampling map having the same destination port group. Within a Standalone UPN flow sampling map pair the forward listing map rules will be applied before the flow sampling map rules.

## Virtual Port Configuration in Standalone UPN Mode

In Standalone UPN map configuration, the virtual port sending traffic to all the port groups need to be configured in Standalone UPN mode.

To configure the virtual port with Standalone UPN mode, select Standalone UPN when configuring the virtual port.

### Overlap Support

Currently, a GTP packet can be destined to at most one destination tool. You can now receive multiple copies of a GTP packet that are sent to various tools (One copy per tool set).

### GigaSMART Rotational Sampling Support

You can now configure GigaSMART Rotational Sampling in a standalone UPN, with *3GPP node role* for the GigaSMART group as **user** and **mode** as *standalone*. For more details refer to [GigaSMART Rotational Sampling](#).

### Interface Filtering and APN/DNN Filtering

## Interface Filtering

In interface-based filtering, the traffic is filtered based on the interface from where it originates. When a new session is created, the interface information will be extracted and checked against the flow sample or whitelist rules. If there is a match with the flow sample or whitelist rules, the traffic belonging to this session will be forwarded to the corresponding tool ports.

### Supported Platforms:

- GigaVUE-HC3 Gen 2
- GigaVUE-HC3 Gen 3

**Note:** You can configure interface-based filtering only through CLI and not through GigaVUE-FM.

You can configure only the interfaces **S1U**, **S5S8U**, **N3**, and **N9** for interface based filtering. It is not recommended to configure other interfaces such as **Gn**, **S5**, **S1** as they are not applicable for standalone UPN interface-based filtering.

The PFCP packets hit the configured interface rule irrespective of the interfaces from where they are originating.

For interface-based filtering (**S1U**, **S5S8U**, **N3**, and **N9**), you must configure the node role as **Standalone UPN** only. The CLI shows the following error, when you configure other node roles.

**"% S1U, S5S8U, N3 and N9 interfaces can be configured only if the 3gpp-node-role is standalone"**

The interface-based filtering supports the filtering of only GTP-U packets.

The following **Standalone UPN flow ops** report displays the **interface** information in the session table:

```
Joy (config) # sh gsgroup flow-ops-report alias gsg-g3 type flow-filtering gtp-imsi-pattern
IMSIVALUE000000
```

```
=====
```

```
Tunnel[Ver] Interface IP:Tunnel-ID => IP:Tunnel-ID IMSI WL FS ID LB port Pkts Timestamp
```

```
IMEI MSISDN
```

```
EBI:LB[QCI] APN
```

```
=====
```

```
CTRL[1] S1U 10.116.22.6:0xb289ad10 => 10.116.22.76:0x135e0620 IMSIVALUE000000 __ 3
45189089276
```

```
IMEIVALUE0000000 MSISDNVALUE000000
```

```
USER 5 10.116.22.44:0x00338cec => 10.116.22.79:0x535e0625 wap.mnc000.mcc000.+ N A 1 _
```

```
CTRL[2] S5/S8-U 10.254.156.136:0x0fb67d86 => 10.254.165.199:0x5dd70620 IMSIVALUE000000 _
_ 17 57994796676
```

```
IMEIVALUE0000000 MSISDNVALUE000000
```

## APN (Access Point Name)/DNN (Data Network Name) Filtering

The Access Point Name (APN) is the name of a gateway between a 4G or 5G mobile network and another computer network, mostly the public Internet. A mobile device making a data connection must be configured with an APN.

In **APN/DNN** filtering, the traffic is filtered based on the **APN** string matching.

**Note:** You can configure APN/DNN filtering only through CLI.

When a new session is created, the **APN** pattern will be extracted and checked against the flow sample or whitelist rules, if there is a match with the **APN** pattern, the traffic belonging to this session will be forwarded to corresponding tool ports. In case of 5G traffic, the **DNN** information will be processed under the **APN** identifier.

The pattern match can be supported as an independent filtering or can be combined with the other filtering parameters such as the IMSI/IMEI/MSISDN.

The **APN/DNN** filtering supports the filtering of both the PFCP and GTP-U packets.

The following **Standalone UPN flow ops** report displays the **APN/DNN** information in the session table:

```
Joy (config) # sh gsgroup flow-ops-report alias gsg-g3 type flow-filtering gtp-imsi-pattern
IMSIVALUE000000
```

```
=====
=====
```

```
Tunnel[Ver] Interface IP:Tunnel-ID => IP:Tunnel-ID IMSI WL FS ID LB port Pkts Timestamp
```

```
IMEI MSISDN
```

```
EBI:LB[QCI] APN
```

```
=====
=====
```

```
IMSIVALUE000000 _ 0 0
```

```
IMEIVALUE0000000 MSISDNVALUE0000
```

```
CTRL 10.241.15.8 : 0x21480840 => 10.241.15.36 : 0x158a2740
```

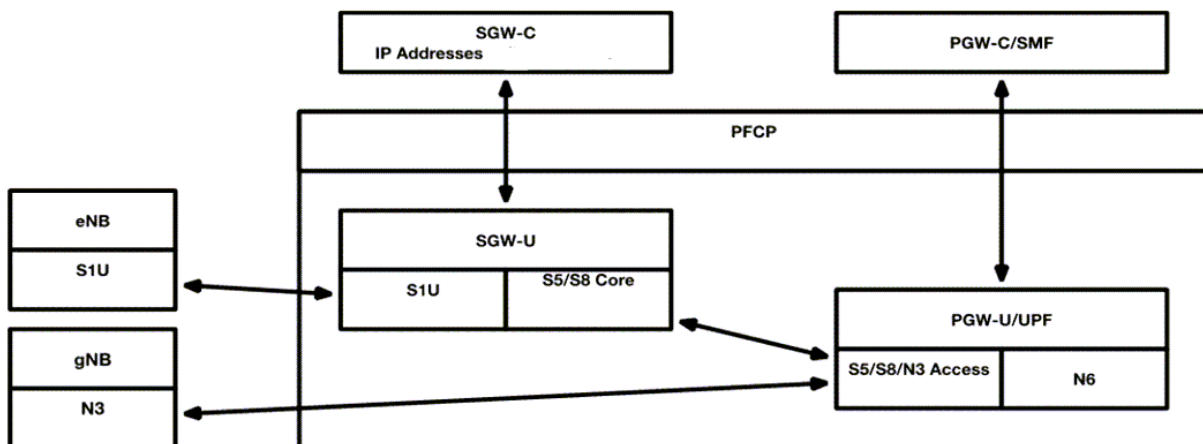
```
USER(S5S8U) 10.226.162.249:0x04f82ea1 => 0.0.0.0:0x00000000 ims.mnc000.mcc000.gp+ N A 2
```

```
USER(S5S8U) 0.0.0.0:0x00000000 => 10.241.15.41:0x558a2745 ims.mnc000.mcc000.gp+ N A 2
```

```
=====
=====
```

## Custom Interface Selection

When the interface IE is not available in the PFCP packets, you can explicitly provide the IP addresses of the network nodes such as SGW-C and SGW-U for identifying and filtering the traffic based on the interface (S1U, S5S8-U and N3). To configure customer interface selection, refer the [Configure Custom Interface Selection](#) topic.



### Supported Platforms:

- UPN in GigaVUE-HC3 Gen 2 GigaSMART Card
- UPN in GigaVUE-HC3 Gen 3 GigaSMART Card

**NOTE:** This feature can be configured only through the GigaVUE-OS CLI and not through the GigaVUE-FM.

A new gsparm is introduced in the GigaVUE-OS CLI, which enables you to choose between the custom interface filtering option and the default 3GPP interface type IE based filtering and populate an IP address profile. As part of the profile configuration, you must enter the range of IP addresses associated with SGW-C and access IP addresses associated with S5S8-U in the GigaVUE-OS CLI.

### Configuration of custom interface selection through CLI

- This feature is supported on gsgroup 3gpp-node-role user mode stand-alone.
- The custom mode must be enabled in the upn-interface-select gsparms and an IP profile must be attached.
- The newly added gsparm will take 3GPP Interface filtering as the default option.
- When upgrading to software release version GigaVUE 6.5.00, the N4/N3 user traffic will not be correlated and will be discarded since the QFI value will not be preserved through persistence records.
- Multiple IP profiles can be created, but only one IP profile can be associated per gsgroup.

- Interface qualifiers that are configured in second-level map rules are not applied to PFCP packets. Instead, PFCP packets will be matched against other configured rule qualifiers. This allows the tool to learn about all PFCP sessions. This approach facilitates session handovers between N3 and S5/S8 by processing PFCP independently of the interface qualifiers. For example, with the flow sample rule "add imsi 1234\* interface N3 percentage 100," packets are handled as follows:

- PFCP Packet 1 (IMSI 1234111111111111 interface N3) matches the rule and is sent to the tool.
- PFCP Packet 2 (IMSI 1234222222222222 interface S5/S8u) also matches and is sent to the tool.
- PFCP Packet 3 (IMSI 1234333333333333 interface S1U) matches and is sent to the tool.
- PFCP Packet 4 (IMSI 1111444444444444 interface N3) does not match and is discarded.

Similarly, for the rule "add interface N3 percentage 100," the packets are handled as follows

- PFCP Packet 1 (interface S1U) matches the rule and are sent to the tool.
- PFCP Packet 2 (interface N3) matches the rule and are sent to the tool.
- PFCP Packet 3 (interface S5/S8u) matches the rule and are sent to the tool.

This demonstrates that the interface criteria is not considered while forwarding the packets.

#### Limitations:

- The IP profile configuration and upn-interface-select gparams is not supported through the GigaVUE-FM.
- The Flow-ops report will not display the interface specific counters for Standalone UPN (S1U, S5S8-U,N3).
- The UPN interface IP list does not support IPv6 addresses. Only IPv4 addresses are supported.
- Once the IP profile is created in the GigaVUE-OS CLI, you cannot modify the IP address or the IP address range specified in the IP profile. You can only create a new profile with a different IP address or IP address range and then associate the IP profile to the gsgroup.
- 

## GigaSMART 5G CUPS

This chapter describes about the GigaSMART 5G CUPS solutions and its operations.

Refer to the following sections for details:

- [Required License : 5G-Correlation and CUPS](#)
- [5G Correlation](#)
- [Stand-Alone User Plane Node Traffic Monitoring](#)
- [Tool Traffic in Multi-Site Scenarios](#)
- [Configure CPN-UPN Communication Solution using Ansible](#)

## Overview

Required License : 5G-Correlation and CUPS

Supported Devices: GigaVUE-HC3 Gen 2, and GigaVUE-HC3 Gen 3.

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

The GigaSMART 5G CUPS traffic visibility fabric solution provides network visibility across the control and user planes for the 5G stand-alone packet core network. A 5G stand-alone packet core network comprises the following network functions:

- Authentication Server Function (AUSF)
- Access and Mobility Management Function (AMF)
- Data Network (DN), e.g. operator services, Internet access or third party services
- Structured Data Storage network function (SDSF)
- Unstructured Data Storage network function (UDSF)
- Network Exposure Function (NEF)
- NF Repository Function (NRF)
- Policy Control function (PCF)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- User plane Function (UPF)
- Application Function (AF)
- User Equipment (UE)
- (Radio) Access Network ((R)AN)

The following diagram shows the 5G Stand Alone Packet Core Network, in which only the N11, N3, and N4 interfaces are supported:

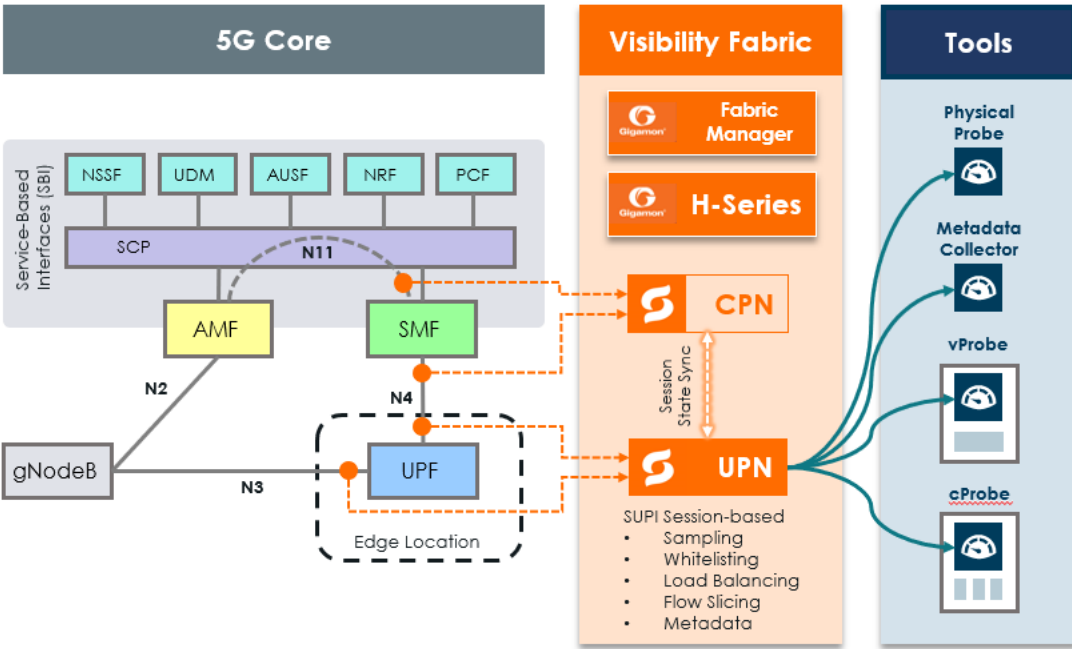


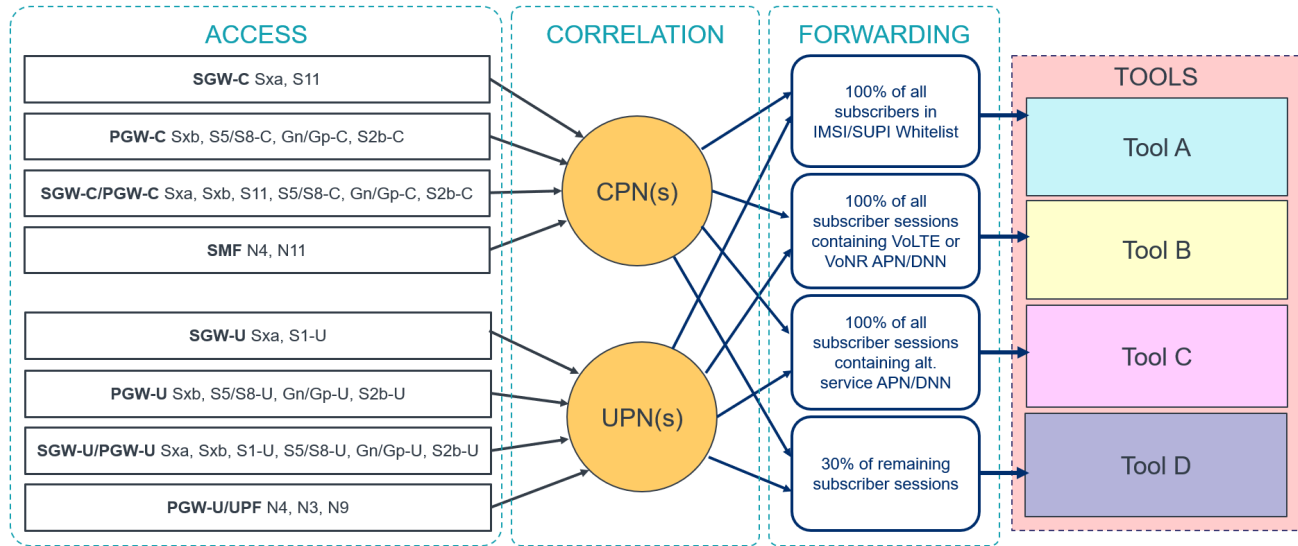
Figure 20 5G Stand Alone Packet Core Network

The GigaSMART 5G CUPS traffic visibility fabric solution has the following three functional areas:

|             |                                                                                                                                                           |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access      | Accesses the traffic through physically or virtually tapping specific interfaces connecting various network element functions.                            |
| Correlation | Subscriber-aware session traffic correlation to enable sending both the control plane portion and user plane portion of a given session to the same tool. |
| Forwarding  | Traffic forwarding through a combination of subscriber-aware white-listing, flow sampling, flow filtering, and load-balancing.                            |

The following diagram explains the LTE and 5G CUPS traffic visibility solution:

## The Essence of CUPS Traffic Visibility Solution



**Note:** the diagram presents an example monitoring scenario based upon specific subscriber aware capabilities, tools and forwarding policy for these tools.

**Figure 21** CUPS Traffic Visibility Solution

In the *Figure 2 : CUPS Traffic Visibility Solution*, specific interfaces of the user plane control functions such as SMF, SGW-C, PGW-C and the user plane functions such as UBF, SGW-U, PGW-U are accessed for getting a copy of the traffic that crosses each interface, and therefore collection of traffic from those access points becomes the basis for traffic monitoring and analysis.

Once the traffic is accessed, it is correlated in order to combine the control plane and user plane traffic for a given subscriber-related session. Then the traffic is forwarded through a combination of white-listing, flow sampling, flow-filtering, and/or load-balancing to traffic monitoring/analysis tools in a load balanced way so that the tools can be used in the most efficient way.

The CUPS solution managed by GigaVUE-FM supports the following mobility networks scenarios based on visibility and analytics fabrics:

- 5G stand-alone mobility networks
- 3G/4G LTE mobility networks
- Mix 3G/4G LTE and 5G mobility networks

## Supported Platforms

GigaSMART 5G CUPS traffic visibility fabric solution is supported in the following platform:

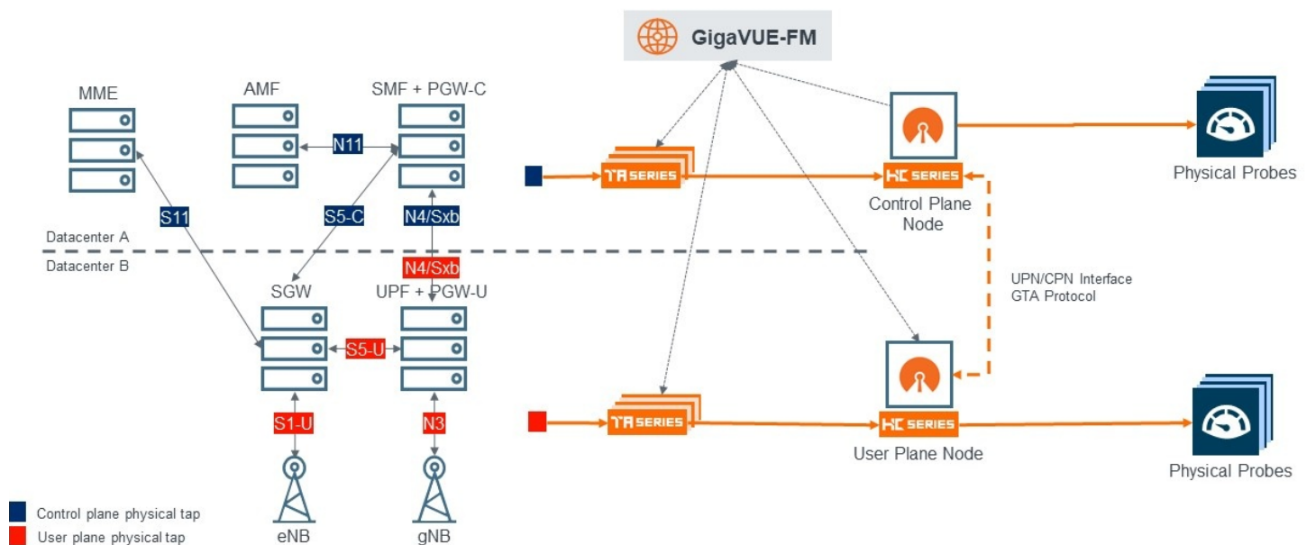
- GigaVUE-HC3

## 5G Correlation

The 5G Correlation feature correlates the 5G Control and User packets to deliver it to different tool ports based on the filtering policies configured. The control and user packets are processed in Control Plane Network (CPN) and User Plane Network (UPN) located in same or different locations, and then the packets are sent to the tools. The following diagram shows the High-Level LTE / 5G CUPS Visibility Environment.

**NOTE:** It is recommended that you unconfigure and reload the GigaSMART card when configuring a particular GS group with 5G and switching back to 4G or vice versa.

### High-Level LTE-CUPS / 5G Visibility Environment



## 5G Load Balancing

If the node role is CPN, the load balancing of the packets depend upon the parameters configured for TCP in GigaVUE-FM.

The UPN node load balances the correlated packets across all the tool ports based on the configured hash key value such as SUPI, PEI, GSPI.

### Configure 5G Load Balancing

To configure 5G Load balancing, follow these steps:

1. From the left navigation pane, go to **System > GigaSMART > GigaSMART Operations(GSOP)**, and then click **New**.
2. Specify an Alias in the **Alias** field.
3. Click in the **GigaSMART Group** field and select a GigaSMART group.

4. Click in the GigaSMART Operations (GSOP) field and select Load Balance in **TCP Application Parameters**.
5. Specify the parameters. The following table explains the parameters for configuring the load balancing in CPN:

| TCP Application Parameters | Options                                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application                | <ul style="list-style-type: none"> <li>Broadcast - All the TCP handshake packets are broadcasted to the tool ports in all the maps.</li> <li>Drop - All the unknown application packets of 5G are sent to the collector.</li> <li>Enhanced -</li> </ul>     |
| Load Balance               | <ul style="list-style-type: none"> <li>Enable - All the 5G control packets will be load balanced across the port-groups configured in the flowsampling and whitelisting maps.</li> <li>Disable - All the 5G control packets will be broadcasted.</li> </ul> |
| TCP Control                | <ul style="list-style-type: none"> <li>Broadcast - All the tcp handshake packets will be broadcasted to the tool ports in all the maps..</li> <li>Drop - All the TCP handshake packets will be sent to collector if configured</li> </ul>                   |

## 5G RAN Correlation

A Radio Access Network (RAN) is part of a telecommunications system that connects individual radio devices to the core mobile network through radio connections.

RAN uses GTP and / or 5G correlation. It exposes RAN data fields from control plane (S11), for example:

- New Radio Cell Global Identifier (NCGI)
- Tracking Area Identity (TAI)
- Tracking Area Code (TAC)

The Tracking Area Identity (TAI) and New Radio Cell Global Identifier (NCGI) are extracted from the User location Information (ULI) and sends them to flow sampling, filtering and forward listing.

The RAN correlation for 5G CUPS flow sampling uses the NCGI, TAC and PLMN-ID values.

For 5G RAN based forward listing requires NCGI includes the PLMN Id and the New Radio Cell Global Identifier (NCGI).

RAN data fields are available for correlation, flow sampling and forward listing. It does not support classic flow filtering.

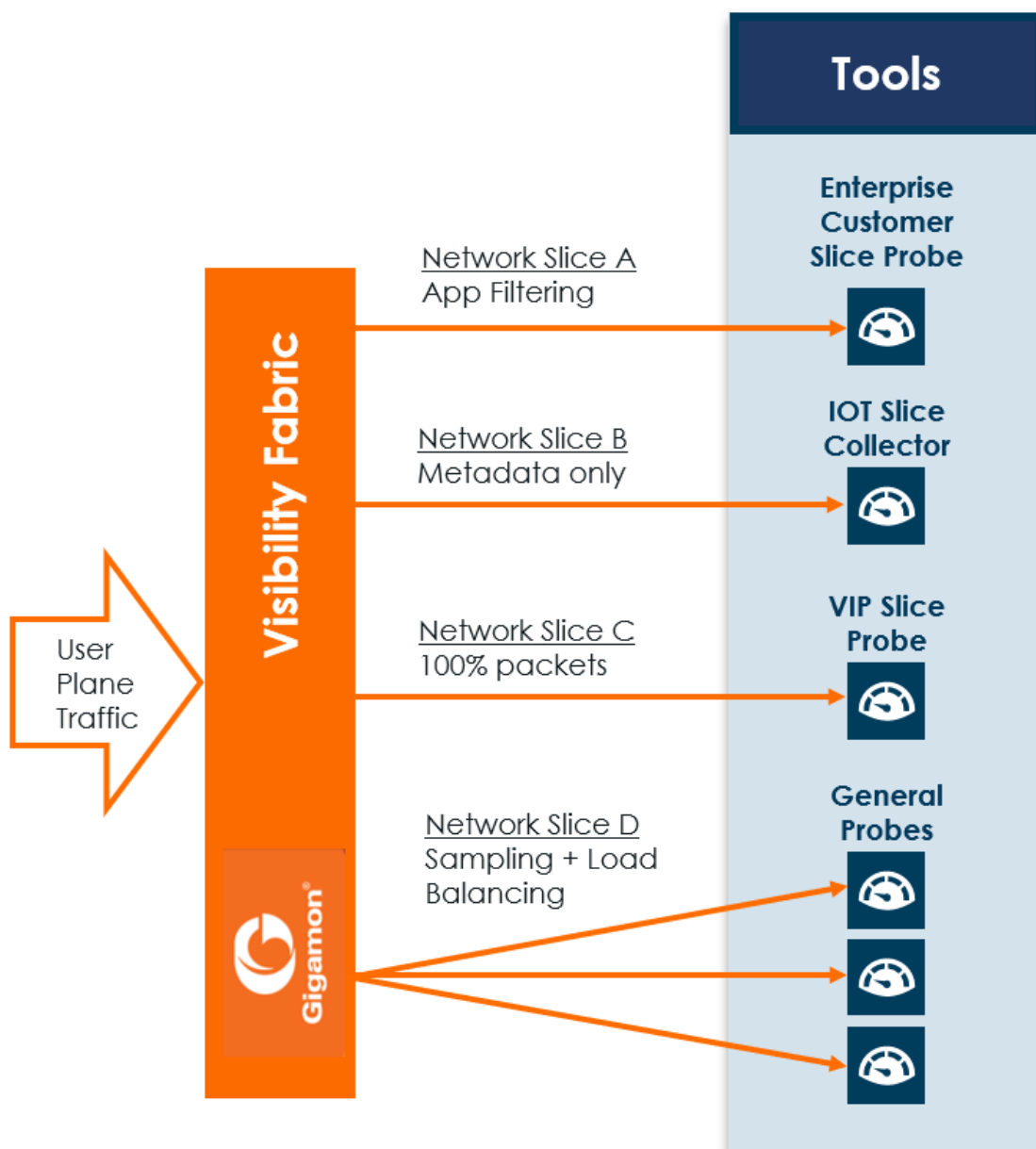
## Configure 5G RAN Correlation

To configure 5G RAN Correlation, refer to [Configure CPN-UPN Communication Solution using Ansible](#)

Refer [Deploying RAN Correlation for Forwarding Subscriber's Traffic Based on Geolocation](#) for more detailed information.

## 5G Network Slice Correlation

Network Slicing is a feature of 5G networks whereby slices of network resources are dedicated to a specific application. Gigamon enables to have differentiated levels of visibility for each network slice.



5G Network Slice Correlation uses 5G Correlation. It exposes Network Slice instance ID (NSI). NSI is available for filtering through flow sampling maps. 5G subscriber aware filter includes the Network Slice Selection Assistance Information (NSSAI) value for 5G correlation.

## Configure 5G Network Slice Correlation

To configure 5G Network Slice Correlation, refer to [Configure CPN-UPN Communication Solution using Ansible](#)

## 5QI Correlation

In 5G traffic, 5QI values present in the control traffic and its associated QoS Flow Identifiers (QFI) value are correlated and the data traffic is sent to the tools. QoS Flow Identifiers (QFI) identifies each QoS (Quality of Service) flows.

5QI flow sampling are performed based on the QoS flows instead of using other subscriber filtering parameters such as SUPI, PEI, GPSI, DNN.

You can configure 5QI along with other filtering parameters such as SUPI, PEI, GPSI, DNN, NSSAI.

## Rules and Notes

Keep in mind the following rules and notes when you work with the 5QI sampling:

- 5QI does not support whitelisting.

### 5G Flow Sampling and Filtering

**Required License :** FlowVUE license is required for Flow Sampling

5G flow sampling samples a configured percentage of 5G sessions. 5G flow sampling uses map rules to select subscribers and then forward a percentage of the packets to tool ports.

Pass rules are defined in flow sampling maps. Each rule contains some combination of SUPI, PEI, and GPSI numbers or patterns as a percentage to sample. The flow is sampled to see if it matches a rule. The percentage of the subscriber sessions matching each rule are selected.

Map rules specify the type of traffic to be flow sampled by that map. For each new session, map rules are evaluated in top-down order of decreasing priority. If there is a match, the indicated percentage of the subscriber session is either accepted or rejected. If accepted, the traffic is sent to the tool port or Load Balancing group specified in the map. If rejected, the traffic is dropped. If there is not a match to a rule, the traffic is passed to subsequent maps.

## About Flow Sampling Rules and Maps

Flow sampling rules are configured in maps called flow sampling maps. Up to ten (10) flow sampling maps per GigaSMART group are supported. Each flow sampling map supports up to 100 flow sampling rules, for a maximum of 1000 (10\*100) rules per GigaSMART group.

5G flow sampling (rule-based flow sampling) is performed after 5G whitelist-based forwarding. So, flow sampling maps have a priority lower than forward list maps and higher than flow filtering maps.

**NOTE:** For 5G second level maps, a maximum of fifteen maps can be attached to a vport. For example, for the same vport you can have one forward list map and ten flow sampling maps, or ten forward list map, four flow sampling maps, and one flow filtering map. In addition, you can have a collector map, which is not counted.

In the flow sampling maps, the rules in the first map have a higher priority than the rules in the second, third, and subsequent maps. Within any single map, rules are evaluated in order.

Rules can be added to, deleted from, or inserted into a flow sampling map when the subtype selected for a Second Level map is Flow Sample. Suffix wildcarding, such as SUPI 100\*, is supported in the flow sampling map rules.

Use the Add a Rule button in the Maps page to add a new flow sampling rule (a pass rule). Specify SUPI, PEI, or GPSI subscriber IDs, as well as the percentage of the flow to be sampled. The percentage is a range from 1 to 100%. Use 0% to drop sampled data.

A DNN pattern can be specified in a rule by itself.

For DNN, specify a pattern (a name) to match, for example, three.co.uk. Wildcard prefixes and suffixes are supported, for example, \*mobile.com or \*ims\*. The pattern can be specified in up to 100 caseinsensitive alphanumeric characters and can include the following special characters: period (.), hyphen (-), and wildcard (\*).

Use DNN to send traffic that matches a certain DNN pattern to specified tool ports, based on the sampling percentage.

When creating Flow Sampling rules on the Maps page, the first rule created has the highest priority and the priority of subsequent rules is in the order that they are added.

### Add Rule to Flow Sampling Map

Flow sampling is applied for new subscribers. When a new rule is added to the rules in a flow sampling map, traffic will be sent to the port or load balancing group specified in the map.

## Delete Rule from a Flow Sampling Map

When a rule is deleted from a flow sampling map, the session associated with the rule stays active. The traffic associated with the rule will not be reevaluated by subsequent maps.

## Change Priority of Flow Sampling Maps

Priority is set as per the order defined in the policy YAML file within the type.

## Delete Flow Sampling Map

When a flow sampling map is deleted, the priority of the remaining flow sampling maps will be reprioritized. For example, if the first flow sampling map is deleted, the second flow sampling map will increase in priority.

For the deleted flow sampling map, the traffic associated with the rules in the map will be reevaluated and then passed to subsequent maps. When a flow sampling map is re-prioritized, the existing sessions will be reevaluated according to the new priority of the map. The traffic associated with the rules in the map will be reevaluated and then passed to subsequent maps.

When the last flow sampling map is deleted, the traffic associated with the rules in the map will also be reevaluated before being passed to subsequent maps. But the traffic associated with the rules in maps that were not matched, will not be reevaluated because that traffic was already passed to subsequent maps.

## Flow-Ops Report Limitation for Multiple Flow Sampling Maps

The flow-ops report displays the flow sampling rule ID for sessions that have been accepted or rejected by the flow sampling map.

However, since rule IDs are not unique across maps, when there are multiple flow sampling maps, the flow-ops report is unable to identify the exact rule that the session matched. For example, with multiple flow sampling maps, each map can have a rule ID of 1. The rule ID will be identified in the flow-ops report, but not the map associated with it.

## 5G Flow Sampling Percentage

The sampling Percentage field in a map for 5G flow sampling, represents the percentage of subscribers that will be sampled (not the sessions).

The 5G correlation engine tracks all the subscribers and all of their sessions that it sees on the network. In this example, for those subscribers with an SUPI starting with the value 46\*, the 5G correlation engine keeps a list of them and randomly selects 80% of those subscribers and sets them to be in the sample, which means that a tool port (or load balanced group) will see 100% of the packets for 100% of the sessions for those randomly selected 80% of subscribers.

For the other 20% of subscribers, the 5G correlation engine continuously tracks those subscribers through the network but does not send any packets to the tool port (or load balanced group).

## Drop Unmatched Traffic

When a session matches one of the configured flow sampling rules, it is either accepted for sampling or rejected.

If it is accepted, all packets belonging to that 5G session are sent to the tool port or ports specified in the flow sampling maps. If a subscriber is in the sample, then both the control plane packets, and the user-data plane packets are sent to the tools.

If it is rejected, all packets belonging to the session are dropped. If the subscriber is not in the sample, then neither the control plane packets, nor the user-data plane packets are sent to the tools.

Control plane and user-data plane traffic are treated the same. For a matching session, all the control plane and user-data plane traffic will be accepted. Otherwise, all the control plane and user-data plane traffic will be rejected and dropped.

## GTP Overlap Flow Sampling for 4G and 5G

GTP Overlap Flow Sampling for 4G and 5G enables tools to receive their own copy of traffic, through independent evaluation of second level maps. In this overlap mode, if a packet matches a map rule, such as for tool A, that packet is still available to be matched again in subsequent maps, such as for tool B and tool C. The multiple copies of a GTP packet are sent to multiple destinations simultaneously. This applies to both GTP forward listing and GTP flow sampling even if sampling is not employed.

The destination could be a single tool port, a GigaStream or an IMSI based load balanced tool port/GigaStream for a particular tool set. The GigaStream sends traffic to various links, connected to an external load balancer that would be connected to multiple tools.

## Configure GTP Overlap Mapping

The configuration of GTP whitelisting and GTP flow sampling maps that are part of the GTP overlap flow sampling map group follow the same configuration considerations discussed previously in [GigaSMART GTP Whitelisting and GTP Flow Sampling](#). As is the case with regular non-overlap GTP mapping, GTP forward listing selects specific subscribers based on IMSI, whereas GTP flow sampling uses map rules to select subscribers and then forward a percentage of the packets to tool ports.

### Configuration Considerations

This section details certain configuration considerations that apply only to the configuration of GTP forward listing and flow sampling maps for GTP overlap flow sampling maps.

#### About GTP Overlap Flow Sampling Map Mode and Port Groups

A second level type map specifying GTP overlap flow sampling map mode must be selected to configure GTP forward listing and flow sampling maps.

To configure a GTP whilelisting map in overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Whitlelist Overlap** in a map.

To configure a GTP flow sampling map in GTP overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Sample Overlap** in a map .

You can configure one GTP forward listing map and one GTP flow sampling map pair that contain traffic policies corresponding to one destination port group. The load balanced port groups can contain a single port, a port range, or a GigaStream. Note that port groups used in GTP overlapping maps support GigaStream.

The maximum number of port groups per single GTP overlap flow sampling map group is six.

For more information about port groups, refer to [Port Groups](#).

#### Maximum Number of Port Group Members

The Maximum number of port group members can be determined as follows:

##### Standalone Configuration

In a standalone configuration, use the following sequence :

1. Determine the number of members per port group and add 1.

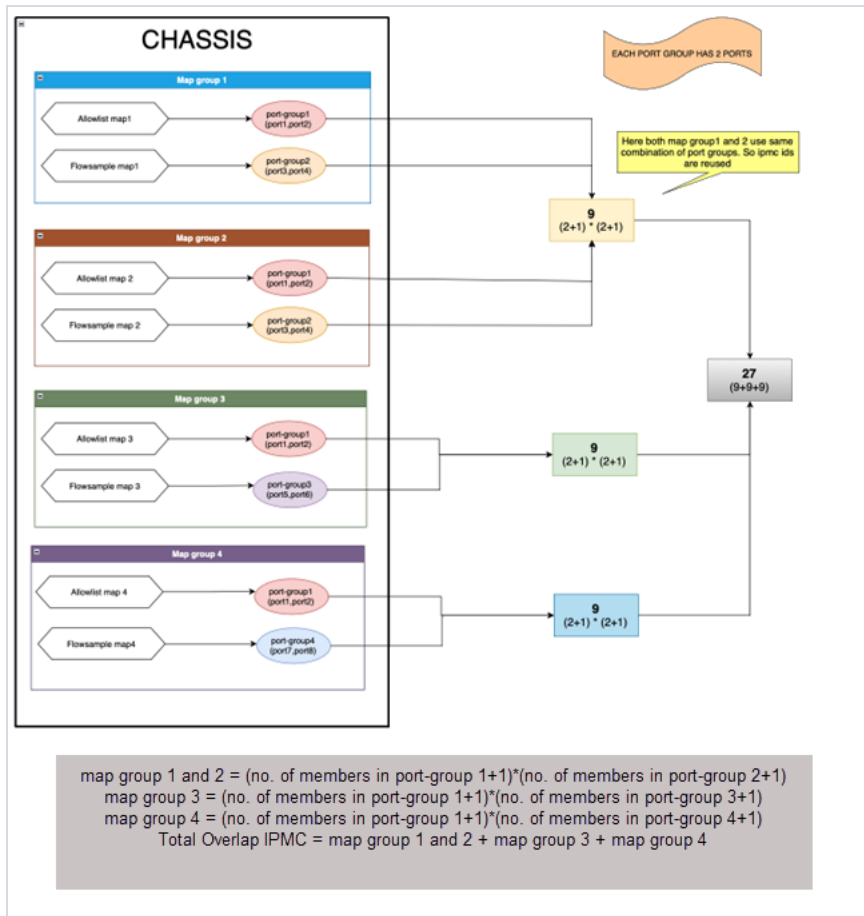
2. Multiply each port group result by each other.
3. The total multiplication should not exceed 4096.

For instance, assume the following configuration in a GTP overlap mapping group:

- o Port Group 1–2 load-balanced GigaStream
- o Port Group 2–3 load-balanced GigaStream
- o Port Group 3–1 load-balanced tool port
- o Port Group 4–1 load-balanced GigaStream
- o Port Group 5–4 load-balanced tool ports. The total number becomes:  $(2+1) \times (3+1) \times (1+1) \times (1+1) \times (4+1) = 240$

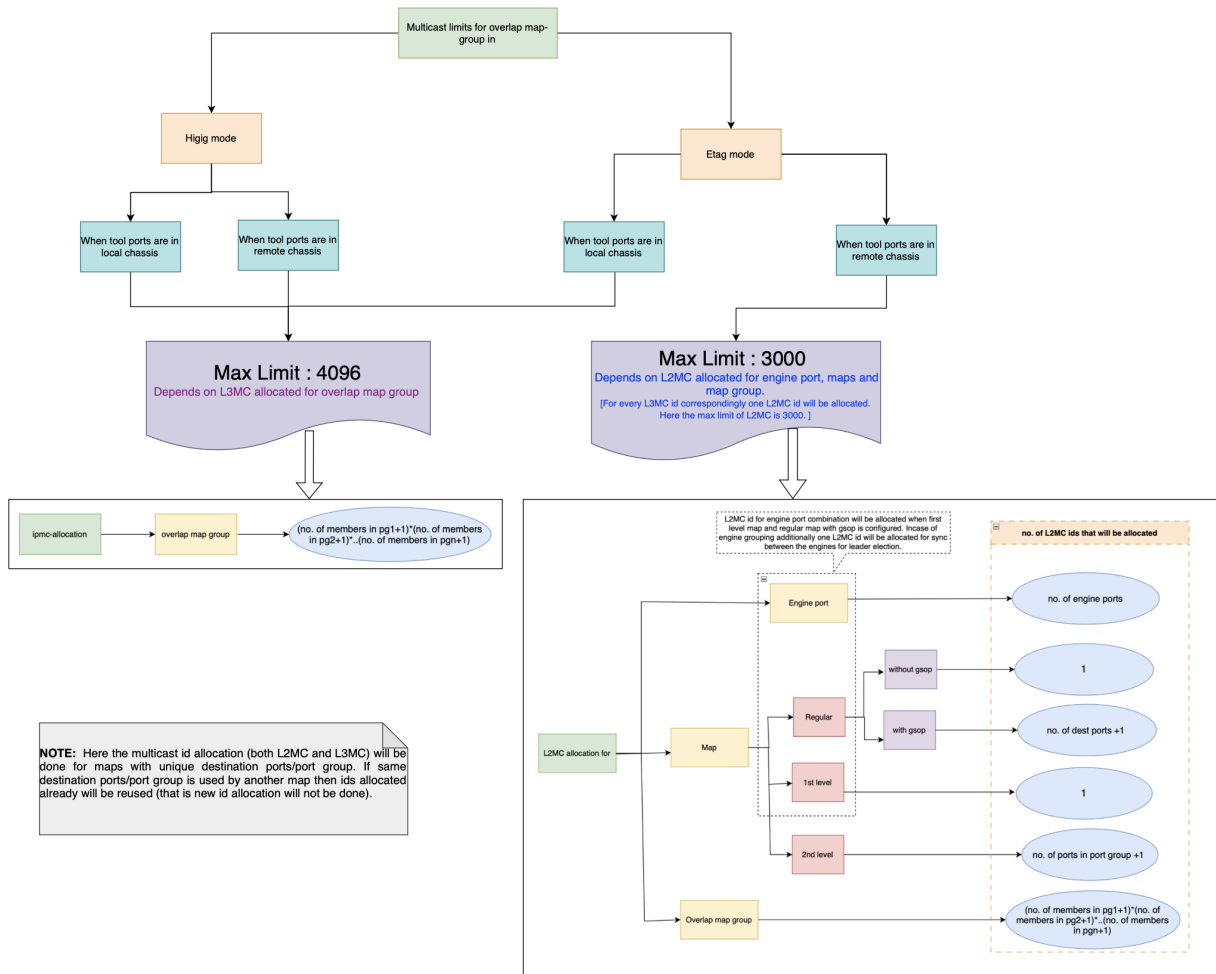
The tool configuration shown is accepted since this does not exceed the maximum number of multicast IDs (4096).

If Port Groups are utilized across multiple map groups in a single cluster, refer to the representation below on how the multicast IDs are calculated.



## Cluster Configuration

In a cluster configuration, Multicast IDs can defer based on Hi-Gig mode or E-tag mode. The below is representation of the same.



## GTP Overlap Flow Sampling Map Priority

A GTP overlap flow sampling map pair consists of one GTP forward listing map and one GTP flow sampling map having the same destination port group. Within a GTP overlap flow sampling map pair the forward listing map rules are applied before the flow sampling map rules.

## Virtual Port Configuration in GTP Overlap Mode

In GTP Overlap map configuration, the virtual port sending traffic to all the port groups needs to be configured in GTP overlap mode.

To configure the virtual port with GTP overlap mode, select **GTP Overlap** when configuring the virtual port.

## About Map Groups

To create a group of maps for GTP forward listing and GTP flow sampling, select **Maps > Maps > Map Groups**, and then click **New**. The maps for a map group are entered in the **Maps** field. All the maps in a map group receive traffic according to map rules, rather than map priority. Thus, multiple copies of a GTP packet can be sent to more than one tool.

The **Maps** field of the Map Group page groups the forward listing and flow sampling maps.

Keep in mind the following configuration considerations for map groups:

- A map group can be associated with only one GigaSMART group (gsgroup).
- All maps within a map group must be connected to the same vport.
- A map group can consist of only one GTP whitelisting map or only one GTP flow sampling map but it cannot contain two maps of the same type.
- Once a map group is created, it cannot be edited to change the type or subtype of the map. However, you can add and edit the map rules for a map while it is configured in a map group.

For more information about map groups, refer to [Create Map Groups](#).

## About Whitelist Maps

The GTP forward list is an IMSI list which is common to all whitelist maps. You can configure an optional rule within a whitelist map to specify a GTP version or interface-based policy.

Other than specifying a new second level type using **Type Second Level** and **Subtype Flow Whitelist Overlap** when creating the map, the configuration of GTP whitelist maps follows the same configuration guidelines as given in the section [GTP Whitelisting](#).

A maximum of six whitelist maps sending traffic to six different port groups can be configured per GigaSMART group (gsgroup).

## About Flow Sampling Maps

In GTP overlap flow sampling map mode, GTP flow sampling (rule-based flow sampling) is performed after GTP whitelist-based forwarding. Therefore, flow sampling maps have a lower priority than whitelist maps. Thus, within a GTP overlap map pair that consists of a single GTP forward list overlap map and a GTP flow sampling overlap map, the GTP whitelist map is of higher priority.

Within the flow sampling maps, the rules in the first map have a higher priority than the rules in the second, third, and subsequent maps. Within any single map, rules are evaluated in order.

A maximum of six flow sampling maps sending traffic to six different port groups can be configured per GigaSMART group (gsgroup).

Within each GTP forward listing and flow sampling pair, if there is not a match to an IMSI in the whitelist map, the traffic flow is sampled based on the rules in the flow sampling map. The flow sampling rules specify IMSI, IMEI, and MSISDN numbers, as well as the percentage to sample.

Within each map pair, packets are then accepted or rejected. Accepted packets are forwarded to the port groups for load balancing. Rejected packets are dropped.

Use the following steps to configure

| Task | Description                                                                                                                          | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Create GigaStreams that will be part of the port groups                                                                              | <ol style="list-style-type: none"> <li>Select <b>Ports &gt; Port Groups &gt; GigaStreams</b></li> <li>Click <b>New</b>.</li> <li>Enter the name in the Alias field.</li> <li>In the Ports field, select port.</li> <li>Click <b>Save</b>.</li> <li>Configure a second GigaStream with the alias, select the required ports in the Ports field, and click <b>Save</b>.</li> </ol>                                                                                                                                                                                      |
| 2    | Create port groups and specify the tool ports and assign GigaStreams to the port groups. The port groups will also be load balanced. | <ol style="list-style-type: none"> <li>Select <b>Ports &gt; Port Groups &gt; All Port Groups</b>.</li> <li>Click <b>New</b>.</li> <li>Enter the name in the Alias field.</li> <li>Select Type GigaSMART Load Balancing.</li> <li>In the Ports field, select ports.</li> <li>In the GigaStream field, select the required GigaStream.</li> <li>Click <b>Save</b>.</li> <li>Configure a second Port Group. with the alias, select ports and in the Ports field, select GigaSMART Load Balancing, select in the GigaStream field, and then click <b>Save</b>.</li> </ol> |

| Task | Description                                                                                                                            | UI Steps                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | Configure a GigaSMART group and associate it with a GigaSMART engine port.                                                             | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; GigaSMART Groups.</li> <li>Click <b>New</b>.</li> <li>Enter the name in the Alias field.</li> <li>In the Port List field, select an engine port.</li> <li>Click <b>Save</b>.</li> </ol>                                                            |
| 4.   | <p>Create a virtual port.</p> <p><b>Note:</b> You must enable GTP Overlap when configuring a virtual port for GTP overlap mapping.</p> | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; <b>Virtual Ports</b> &gt; <b>Virtual Ports</b>.</li> <li>Click <b>New</b></li> <li>Enter the name in the Alias field.</li> <li>In the GigaSMART Group field, select the group.</li> <li>Select GTP Overlap.</li> <li>Click <b>Save</b>.</li> </ol> |
| 5.   | Create the GTP Whitelist                                                                                                               | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; <b>GTP Whitelist</b>.</li> <li>Click <b>New</b>.</li> <li>Enter Whitelist in the Alias field</li> <li>Go to Task 6.</li> </ol>                                                                                                                     |
| 6.   | Fetch whitelist files from a specified location to populate the GTP forward list.                                                      | <ol style="list-style-type: none"> <li>On the GTP Whitelist page, select Bulk Upload.</li> <li>Select Bulk Entry Operation for IMSI Upload Type.</li> <li>Select Upload from URL from the Bulk Upload Type list.</li> <li>Enter the URL in the Enter Remote URL field.</li> <li>Click <b>Save</b>.</li> </ol>                         |
| 7.   | Associate the GigaSMART group to the GTP forward list.                                                                                 | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups</li> <li>Select GS Group GS31 created in Task 3 and click Edit</li> <li>Under GTP Whitelist, click on the GTP Whitelist Alias field and select Whitelist.</li> <li>Click <b>Save</b>.</li> </ol>            |

| Task | Description                                                                                       | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.   | Configure the GigaSMART operation for GTP forward listing.                                        | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>Click <b>New</b>.</li> <li>Enter the name in the Alias field.</li> <li>Select the GigaSMART Group from the GigaSMART Groups list.</li> <li>Select GTP Whitelist from the GigaSMART Operations (GSOP) list</li> <li>Select Load Balancing from the GigaSMART Operations (GSOP) list.</li> <li>Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>Select Stateful</li> <li>Set Type to GTP</li> <li>Select Hashing</li> <li>Select IMSI</li> </ul> </li> <li>Click <b>Save</b>.</li> </ol> |
| 9.   | Configure the GigaSMART operation for GTP flow sampling.                                          | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>Click <b>New</b>.</li> <li>Enter the name in the Alias field.</li> <li>Select the GigaSMART Group from the GigaSMART Groups list.</li> <li>Select Flow Sampling-GTP.</li> <li>Select Load Balancing from the GigaSMART Operations (GSOP) list.</li> <li>Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>Select Stateful</li> <li>Set Type to GTP</li> <li>Select Hashing</li> <li>Select IMSI</li> </ul> </li> <li>Click <b>Save</b>.</li> </ol>                                      |
| 10.  | Configure the first level maps.<br>In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic. | <ol style="list-style-type: none"> <li>Configure the first map as follows: <ul style="list-style-type: none"> <li>Alias.</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Task | Description                                                                                                                                                                                                                                                 | UI Steps                                                                                                                                                                                                                                                                                                                                                                                             |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Type and Subtype</li> <li>• Source</li> <li>• Destination</li> <li>• Rule 1</li> <li>• Rule 2</li> <li>• Click <b>Save</b>.</li> </ul>                                                                                                                                                                                                                      |
| 11.  | Configure the first second level GTP overlap map for GTP forward listing If there is a match to an IMSI in the forward list for GTP version 1 traffic, it is then forwarded to load balancing port group.                                                   | <ol style="list-style-type: none"> <li>a. Select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click <b>New</b>.</li> <li>c. Configure the map.</li> </ol> <ul style="list-style-type: none"> <li>• Alias</li> <li>• Type and Subtype</li> <li>• Source</li> <li>• Destination</li> <li>• GSOP</li> <li>• Rule 1.</li> </ul> <ol style="list-style-type: none"> <li>d. Click <b>Save</b>.</li> </ol>  |
| 12.  | Configure a second level map for GTP flow sampling, the flow sampling map. If there is not a match to an IMSI in the forward list, the traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to load balancing port group. | <ol style="list-style-type: none"> <li>a. Select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click <b>New</b>.</li> <li>c. Configure the map.</li> </ol> <ul style="list-style-type: none"> <li>• Alias</li> <li>• Type and Subtype.</li> <li>• Source.</li> <li>• Destination</li> <li>• GSOP</li> <li>• Rule 1</li> </ul> <ol style="list-style-type: none"> <li>d. Click <b>Save</b>.</li> </ol> |
| 13.  | Configure the next second level GTP overlap map for GTP forward listing If there is a match to an IMSI in the forward list for GTP version 2 traffic, it is then forwarded to load balancing port group.                                                    | <ol style="list-style-type: none"> <li>a. Select <b>Maps &gt; Maps &gt; Maps</b>.</li> <li>b. Click <b>New</b>.</li> <li>c. Configure the map.</li> </ol> <ul style="list-style-type: none"> <li>• Alias</li> <li>• Type and Subtype</li> <li>• Source</li> <li>• Destination</li> </ul>                                                                                                             |

| Task | Description                                                                                                                                                                                                                                                                                                      | UI Steps                                                                                                                                                                                                                                                                                                 |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• GSOP</li> <li>• Rule 1</li> </ul> <p>d. Click <b>Save</b>.</p>                                                                                                                                                                                                  |
| 14.  | Configure the next second level map for GTP flow sampling. If there is not a match to an IMSI in the forward list as evaluated by the second level GTP whitelisting map <i>WLMAP2</i> , the traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to load balancing port group. | <p>a. Select <b>Maps &gt; Maps &gt; Maps</b>.</p> <p>b. Click <b>New</b>.</p> <p>c. Configure the map:</p> <ul style="list-style-type: none"> <li>• Alias</li> <li>• Type and Subtype: Sample Overlap</li> <li>• Source</li> <li>• Destination</li> <li>• Rule 1</li> </ul> <p>d. Click <b>Save</b>.</p> |
| 15.  | Configure a map group. Add the GTP forward listing and the two GTP flow sampling maps configured in previous steps.                                                                                                                                                                                              | <p>a. Select <b>Maps &gt; Map Groups</b>.</p> <p>b. Click <b>New</b>.</p> <p>c. Enter OverlapMap in the Alias field.</p> <p>d. In the Maps field, select the maps.</p> <p>e. Click <b>Save</b>.</p>                                                                                                      |

## Overlap Map Statistics

Overlap maps are displayed based on the following:

- If at least 1 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 1 pair of maps accepts the packets, the Sample (Tx) counters in the GTP Interface stats is incremented only once.
- If at least 1 whitelist 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 1 pair of maps matches the packets, the Sample (Tx) counters in the GTP Interface stats is incremented only once.
- If there are no WL maps and all flow sample maps are no rule match, then Sample(Tx) and Sample Out counters in the GTP Interface stats is not incremented.

# 5G Stateful Session Recovery

## Required License: 5G Correlation

5G stateful session recovery provides session persistence for GigaSMART 5G applications, including 5G flow filtering, 5G forward listing, and 5G flow sampling. In this method of recovery, 5G sessions are backed up periodically so that they can be recovered faster after a GigaSMART line card reboot or a node reboot.

5G stateful session recovery requires additional memory for storing backups. GigaVUE-HC3 has the required memory.

Using 5G stateful session recovery, the 5G session tables in the GigaSMART line card memory is periodically backed up to the control card memory on the node and stored.

You should configure an interval for how often the backups occur, such as every 10 minutes. If 5G stateful session recovery is enabled and the GigaSMART line card is rebooted, the 5G session tables is restored automatically following the reboot.

The last stored backup file is downloaded from the control card to the GigaSMART line card using FTP. The session table is repopulated from the last stored backup file to each GigaSMART engine, up to 8 engines. Packet count statistics for sessions are saved and restored.

Depending on the size of the session table, the amount of time to restore from the backup might take as much as 3 minutes. During that interval, traffic is blocked to the virtual port on the GigaSMART line card. Once the session table is read and populated, traffic is allowed.

Depending on the interval between backups, there could be differences between the stored state and the current state of the system, for example, map configuration could change, or sessions could be added, modified, or deleted.

Load balancing information is not persisted, so after a session table is repopulated, a session that was once sent to one load balanced port may be sent to a different load balanced port after the reboot. However, for SUPI-based load balancing, the traffic is sent to the same port as it was before the reboot.

5G stateful session recovery works in a cluster environment; however, the cluster leader must remain the same.

## Configure 5G Stateful Session Recovery

To enable 5G stateful session recovery, as well as to configure timers, do the following:



1. On the left navigation pane, click , and then select **Physical>Nodes**.
2. From the device view, select **GigaSMART > GigaSMART groups**.
3. Click on the alias of the **GigaSMART group**.
4. Select **GTP Persistence** in the **GTP Persistence** fields under GigaSMART Parameters as shown in the [Figure 22GTP Persistence GigaSMART Parameters](#). The timers are pre-configured with default values.

▼ GTP Persistence

|                                                            |                                                                                        |
|------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>GTP Persistence</b> <input checked="" type="checkbox"/> |                                                                                        |
| GTP Persistence Interval (minutes)                         | 10  |
| GTP Persistence Restart Age Time (minutes)                 | 30  |
| GTP Persistence File Age Timeout (minutes)                 | 30  |

**Figure 22** *GTP Persistence GigaSMART Parameters*

Use the **System** widget on the Overview page to determine the amount of memory. The size of memory is 24Gb in an upgraded system.

### View Backup and Restore information

To view the System information, select **Overview** from the Navigation pane. The amount of free and used memory is displayed in the **Memory** field.

To view backup and restore information for GTP Persistence:

1. Select **GigaSMART > GigaSMART Groups > GigaSMART Group**.
2. Click on the alias of the GigaSMART group.

A Quick View appears for the selected GigaSMART group.

3. Scroll down to GTP Persistence. In [Figure 23GTP Persistence Information](#), GigaSMART Group gsggrp-1\_4\_e1 is selected and the Quick View is displayed.

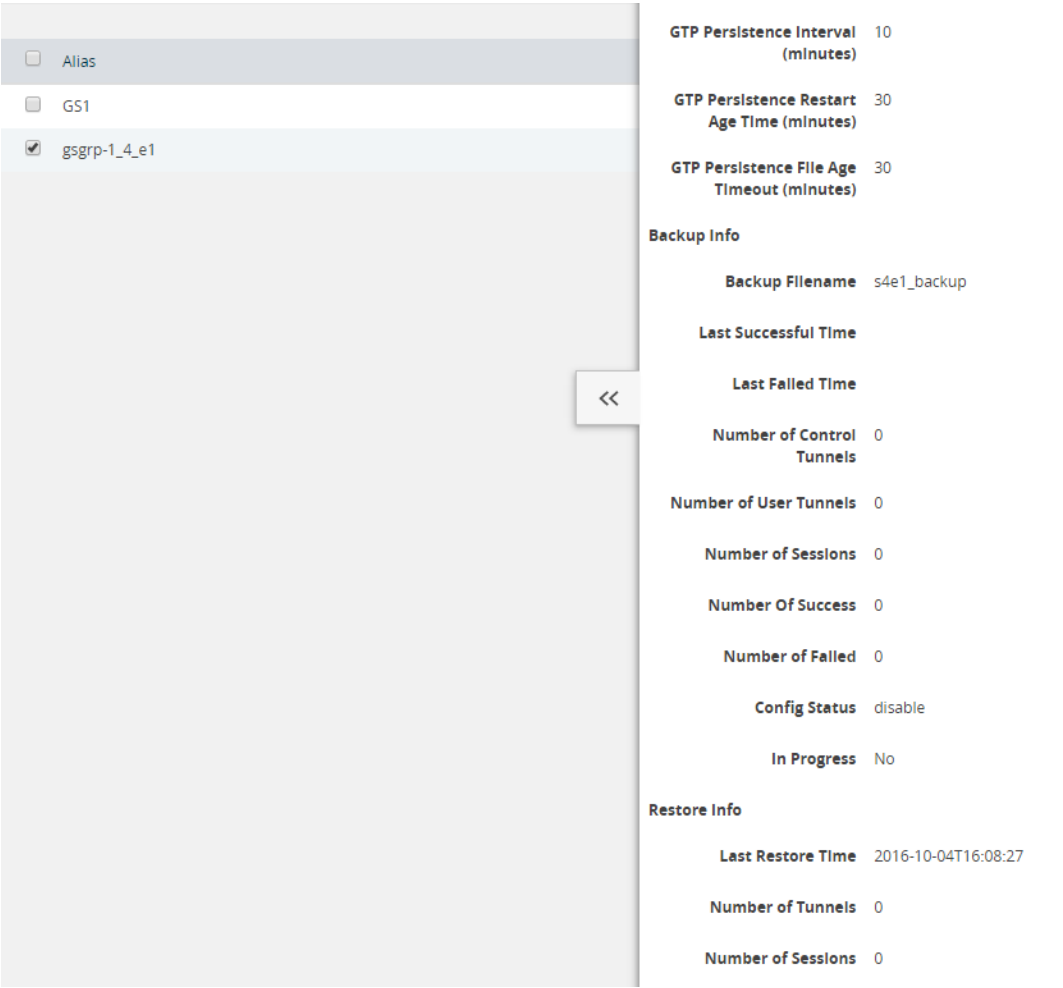


Figure 23 GTP Persistence Information

The following table describes persistence information.

Table 1: GigaSMART GTP Persistence Information

| Name                      | Format                                                       |
|---------------------------|--------------------------------------------------------------|
| Backup Info               |                                                              |
| Backup file name          | The internal name of the backup file.                        |
| Last successful time      | The time stamp of the last successful backup.                |
| Last fail time            | The time stamp of the last failed backup.                    |
| Number of control tunnels | The number of control tunnels backed up.                     |
| Number of user tunnels    | The number of user tunnels backed up.                        |
| Number of sessions        | The number of sessions backed up.                            |
| Number of success         | The number of successful backups.                            |
| Number of failed          | The number of failed backups.                                |
| Config Status             | The status of a backup, which is either Enabled or Disabled. |

| Name                | Format                                   |
|---------------------|------------------------------------------|
| In Progress         | The progress, which is either Yes or No. |
| <b>Restore Info</b> |                                          |
| Last restore time   | The time stamp of the last restore.      |
| Number of tunnels   | The number of tunnels restored.          |
| Number of sessions  | The number of sessions restored.         |

## Remove Backup files

To delete backup files, do the following:

1. Select the alias of GigaSMART Group.
2. Click **Edit**.
3. Scroll down to GTP Persistence (refer to [Figure 24GTP Backup Files Delete](#))
4. Click **Delete All** under **GTP Backup Files**.

▼ GTP Persistence

GTP Persistence ☐

GTP Persistence Interval (minutes) 10

GTP Persistence Restart Age Time (minutes) 30

GTP Persistence File Age Timeout (minutes) 30

GTP Backup Files

Delete All

Figure 24 GTP Backup Files Delete

## 5G Whitelisting

### Required License : 5G Whitelisting

5G Whitelisting selects specific subscribers based on SUPI. The whitelist contains up to 2,000,000 subscriber SUPIs in Gen2 GigaSMART. For subscribers in the whitelist, 100% of their traffic is always sent to a specified tool port.

For example, when a subscriber session comes in, 5G whitelisting checks the SUPI of the subscriber.

If the incoming SUPI matches an SUPI in the whitelist, all sessions associated with that SUPI are sent to the tool port or load balancing group specified in the whitelist map.

## Configure Whitelist Maps

The whitelist maps are configured per GigaSMART group. Each whitelist map, associated with the same vport, uses the same underlying whitelist.

Up to ten (10) whitelist maps are supported. Multiple whitelist maps provide a granular selection of tool ports for whitelisting. Using multiple maps, traffic can be segregated and sent to multiple destinations. Whitelist map rules allow you to select the subset of SUPIs sent to a particular tool.

Each whitelist map can contain up to four rules. The rules specify the type of traffic to be whitelisted by that map. Within any single map, the rules are evaluated in order. The rules in the first map have a higher priority than the rules in the second, third, and subsequent maps.

The rules are specified based on the Data Network Name (DNN). A DNN can be specified in a rule of a Second Level Flow Whitelist map. 5G Whitelist map contains only DNN specific filters.

For DNN, you must specify a pattern (a name) to match. Use DNN to direct the traffic that matches the pattern to a specific tool.

A DNN pattern is for example, three.co.uk. Wildcard prefixes and suffixes are supported, for example, \*mobile.com or \*ims\*. The pattern can be specified in up to 100 case-insensitive alphanumeric characters and can include the following special characters: period (.), hyphen (-), and wildcard (\*). A standalone wildcard (\*) is not allowed for DNN.

Each new subscriber session will be evaluated by the whitelist maps in the order of priority, which, by default, is the order in which the maps were created.

When a subscriber session comes in, 5G whitelisting will check the SUPI of the subscriber. If the SUPI is present in the whitelist, the rules in the first whitelist map is evaluated to qualify the match further. Otherwise, the packet is evaluated against the rules in the subsequent whitelist maps for a possible match.

**NOTE:** Both maps can specify the same destination.

Rules can be added to, or deleted from, a whitelist map. Use the Add a Rule button to add a new whitelist rule (a pass rule). Click x to delete a rule. A rule in a whitelist map cannot be edited. To edit a rule, first delete it, then recreate it.

The default map configuration DNN specified in the map, continues to be supported. If the incoming SUPI matches an SUPI in the whitelist, the session will be sent to the tool port, GigaStream, or Load Balancing group specified in the whitelist map. Whitelist maps cannot contain any other rules such as GigaSMART rules (gsrule), flow filtering rules (flowrule), or flow sampling rules (flowsample).

5G whitelist-based forwarding is performed prior to 5G flow sampling (rule-based flow sampling) and 5G flow filtering.

**NOTE:** For 5G second level maps, a maximum of fifteen maps can be attached to a vport. For example, for the same vport you can have five whitelist maps and ten flow sampling maps, or ten whitelist maps, and five flow sampling maps. In addition, you can have a collector map, which is not counted.

Whitelist maps cannot contain any other rules such as GigaSMART rules (gsrule), flow filtering rules (flowrule), or flow sampling rules (flowsample).

## Change Priority of Whitelist Maps

Priority is set as per the order defined in the policy YAML file within the type.

## Delete Whitelist Maps

When a whitelist map is deleted, the priority of the remaining whitelist maps are re-prioritized.

For example, if the first whitelist map is deleted, the second whitelist map increases in priority.

For the deleted whitelist map, the traffic associated with the rules in the map is reevaluated and then passed to subsequent maps.

When a whitelist map is re-prioritized, the existing sessions are reevaluated according to the new priority of the map. The traffic associated with the rules in the map are reevaluated and then passed to subsequent maps.

When the last whitelist map is deleted, the traffic associated with the rules in the map is also reevaluated before being passed to subsequent maps. But the traffic associated with the rules in maps that were not matched, are not reevaluated because that traffic was already passed to subsequent maps.

When a single whitelist entry is added, whitelisting is applied for new as well as existing subscribers.

When a new whitelist file is fetched, whitelisting is applied only for new subscribers.

Whitelisted traffic is then sent to the port or load balancing group specified in the whitelist map.

Entries in the whitelist can be deleted one at a time. Each entry is a single SUPI.

When a whitelist entry is deleted, the session associated with the whitelist entry stays active and traffic is still sent to the whitelist map. The whitelist session is not reevaluated or passed to subsequent maps.

To delete a single entry from the whitelist, select Individual Entry Operation, refer to Delete GTP Whitelist Maps in [GigaSMART GTP Whitelisting and GTP Flow Sampling](#).

To perform the following, refer to [GigaSMART GTP Whitelisting and GTP Flow Sampling](#):

- Create Whitelist
- Apply Whitelist
- Delete Entry from Whitelist
- Delete Multiple Entries from Whitelist
- Delete Whitelist
- Destroy Whitelist

### **User Plane Node Traffic Monitoring**

In User Plane Node (UPN) traffic monitoring, the UPN processes the subscriber information that is extracted from the Packet Forwarding Control Protocol (PFCP) packets and correlates with the GTP-u traffic without the CPN.

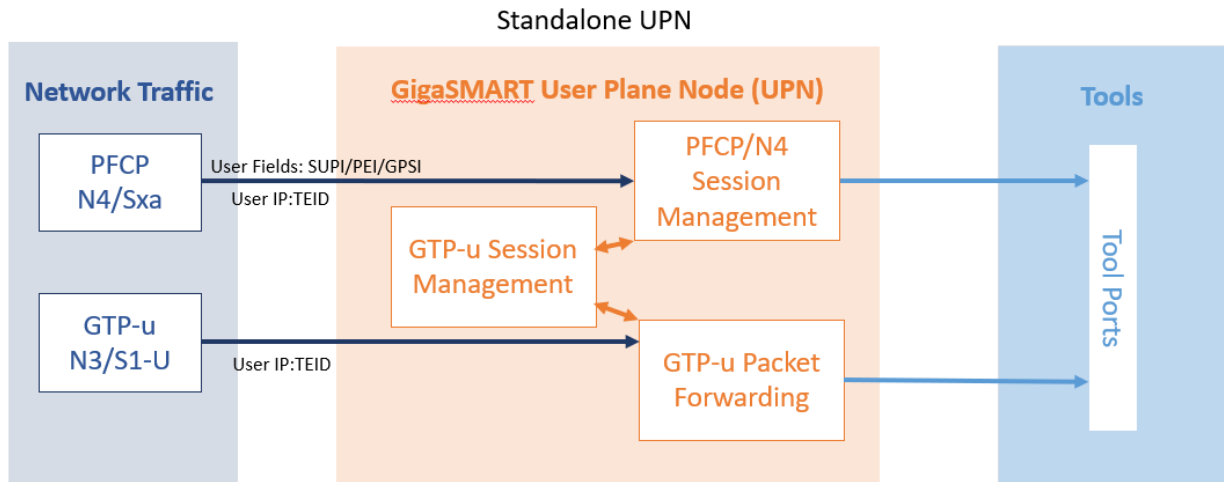
PFCP (Packet Forwarding Control Protocol) is a 3GPP Protocol that is communicated on the Sxa, Sxb, N4 Interface between the Control Plane (CP) elements and User Plane (UP) elements. The CP element programs the UP element with policies on how to forward packets.

PFCP allows an optional Informational Elements (IE) that contains SUPI/IMSI, PEI/IMEI, GPSI/MSISDN information of the Subscriber during PFCP Session Establishment Request. If your network enables these optional information elements, then you can use the Stand-Alone User Plane Node traffic monitoring.

The UPN performs the following activities in the Standalone mode:

- Processes the PFCP session establishment request and extracts the SUPI/IMSI, PEI/IMEI, GPSI/MSISDN User IP and TEID for both end points. The information in the PFCP traffic is used to populate the UPN's session table.
- Correlates GTP-U traffic based on the subscriber information from PFCP. GTP-U look up is correlated based on the IP and TEID .
- When UPN standalone mode is used, forward lists are limited to IMSI/SUPI only, and flowsampling maps for filtering or sampling are limited to IMSI/SUPI and IMEI/PEI. You will not be able to use any other CP fields for filtering or sampling, including APN, DNN, QCI, 5QI, ECGI, NCGI, NSI.

The following diagram explains the functioning of UPN in Standalone mode:



## Rules and Notes

- You can create a Stand-Alone UPN traffic monitoring session only when there is atleast SUPI/IMSI in the user fields.
- The UPN only supports PFCP traffic from Sxa for LTE, N4 for 5G. GTP and 5G maps are required to forward traffic.
- The UPN determines if PFCP is from the N4 interface if it has QFI information.

## Configure Stand-Alone User Plane Node Traffic Monitoring

To configure Stand-Alone User Plane Node Traffic Monitoring, refer to [Configure CPN-UPN Communication Solution using Ansible](#)

**NOTE:** You must enable the stand-alone mode in UPN while creating the solution in Ansible. Once the stand-alone mode is enabled, UPN cannot connect with the CPN, and you cannot change the mode. To change the mode, you need to delete the UPN from the solution and add a new one .

## Control Plane Metadata

The mobility control plane metadata feature is used to support the metadata export in JSON format for each transaction occurring in the 3G/4G/5G network.

The mobility network core control traffic is tapped and mirrored to GTP/HTTP2 GigaSMART engines for correlation. The GTP/HTTP2 correlation engine generates metadata for a transaction. It can either be a GTP transaction for 3G/4G control traffic or an HTTP2 transaction for 5G control traffic. The GTP correlation application supports generating metadata for 3G and 4G network. The 5G CPN application supports generating the control plane metadata for 5G network.

The metadata of subscriber activities is extracted using GTP or 5G correlation. After extraction, the metadata is exported to the data collection center in JSON format.

The records are exported for the following transactions:

For 3G:

- Create PDP
- Update PDP
- Delete PDP

For LTE:

- Create Session
- Delete Session
- Create Bearer
- Modify Bearer
- Update Bearer
- Delete Bearer

For 5G

- Create SM Context
- Modify SM Context
- Release SM Context
- N1 N2 Transfer

By default, values such as IMSI/SUPI, IMEI/PEI, MSISDN/GPSI and APN/DNN are added from the Create record to Modify and Delete records.

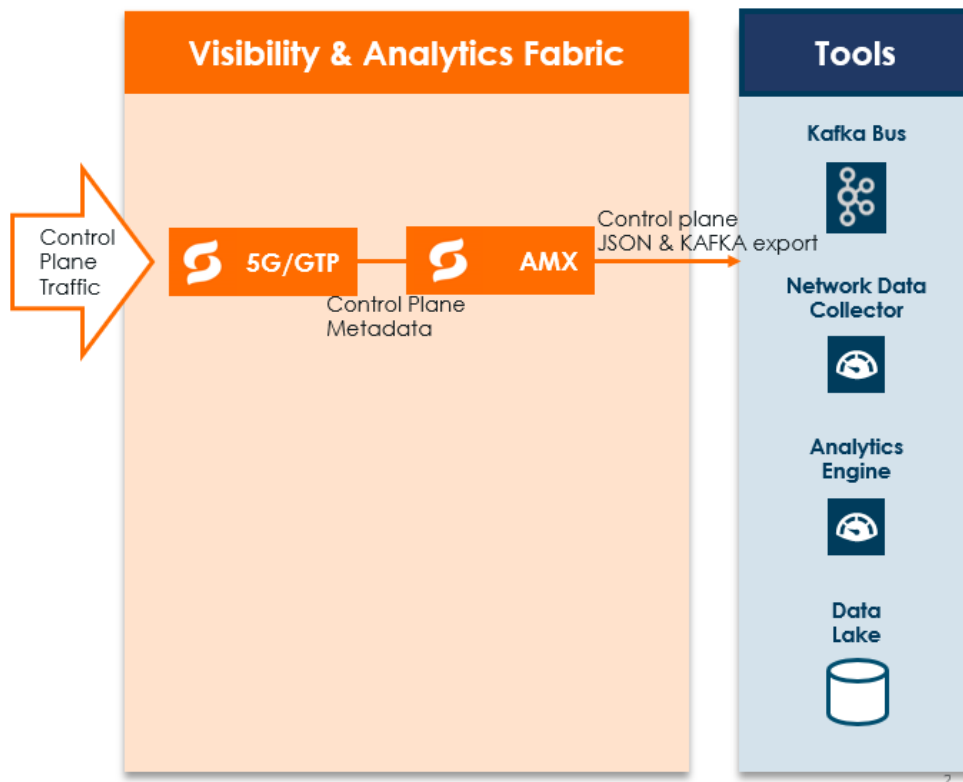
The control plane metadata can be exported in the following two formats:

- Flat
- Hierarchical

The mobility control metadata JSON is encoded from the session table information, current transaction and sent to the AMX application running on GigaVUE V Series Node which is connected at L4 protocol (UDP) level.

Once the transaction is complete in the session table and the metadata is created, it is scheduled for export to AMX. The AMX stores the received mobility control metadata in its internal database and is periodically sent to customer tools either by Kafka bus or as JSON file upload. For information on the export of 3G/4G/5G control plane metadata by AMX, refer [Application Metadata Exporter](#).

**NOTE:** When the 5G subscriber reattaches through the createSMContext before the clean-up is done for the previous user tunnel with the same IMSI and PDU session id, the UE IP address and the Tunnel ID that are populated based on the old user tunnel information will be exported.



### Configuration of 3G/4G Control Plane Metadata using Ansible

To configure 3G/4G control plane metadata, perform the following steps:

| S.No | Steps                        | Refer to..                                   |
|------|------------------------------|----------------------------------------------|
| 1.   | Creating Inventory Directory | <a href="#">Creating Inventory Directory</a> |
| 2.   | Creating <i>fmlInfo.yml</i>  | <a href="#">Creating fmlInfo.yml</a>         |

| S.No | Steps                               | Refer to..                                                           |
|------|-------------------------------------|----------------------------------------------------------------------|
| 3.   | Creating <i>ansible_inputs.json</i> | <a href="#">Creating ansible_inputs.json</a>                         |
| 4.   | Creating 3G/4G inventory file       | <a href="#">Creating 3G/4G control plane metadata inventory file</a> |
| 5.   | Creating <b>host_vars</b> directory | <a href="#">Creating host_vars directory</a>                         |
| 6.   | Creating <b>host_vars</b> files     | <a href="#">Creating host_vars files</a>                             |

## Creating Inventory Directory

Create an Inventory Directory to store all the 3G/4G control plane metadata related configuration files.

```
username@fmreg26:~$ mkdir CP-Metadata-Solution
username@fmreg26:~$ ls -l
drwxr-xr-x 2 ddaniel fmtaf 4096 May 11 11:59 CP-Metadata-Solution
```

## Creating fmInfo.yml

Create fmInfo.yml file inside the Inventory Directory that contains the information such as ip-address, username and password. To create the file, refer to [Schema](#).

## Creating ansible\_inputs.json

Create 'ansible\_inputs.json' file inside the Inventory Directory.

```
gigamon@fmreg26:~/CP-Metadata-Solution $ ls -l
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

File name: ansible\_inputs.json To create a file, refer to [Schema](#).

## Creating 3G/4G control plane metadata inventory file

Create the **mobility\_inventory** file inside Inventory Directory.

```
gigamon@fmreg26:~/CP-Metadata-Solution$ touch mobility_inventory
gigamon@fmreg26:~/CP-Metadata-Solution$ ls -l
```

```
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
```

```
-rw-r--r-- 1 gigamon fmtaf 396 May 11 14:22 mobility_inventory
```

```
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

The file contains the details of the following groups and provide the inputs to the groups as shown in the following table:

| S.No                                                                                                                                      | Groups-Input                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Note:</b> –You can provide the input or leave the field empty if you don't want to use the playbook to configure the following groups. |                                                                                                                                  |
| 1.                                                                                                                                        | <b>Ports</b> —Name of the Cluster or standalone device IP that contains the ports that need to be configured.                    |
| 2.                                                                                                                                        | <b>IPInterfaceSolution</b> —Name of the Cluster or standalone device IP on which the IPInterfaceSolution needs to be configured. |
| 3.                                                                                                                                        | <b>Tool Groups</b> —Name of the Cluster or standalone device IP on which the ToolGroup needs to be configured.                   |
| 4.                                                                                                                                        | <b>GigaStreams</b> —Name of the Cluster or standalone device IP on which the Gigastreams needs to be configured.                 |
| 5.                                                                                                                                        | <b>GTPWhitelist</b> —Name of the Cluster or standalone device IP on which the GTPWhitelist database needs to be configured.      |
| 6.                                                                                                                                        | <b>Policies</b> —Name of the Global policy or policies.                                                                          |
| 7.                                                                                                                                        | <b>GTP</b> — Name of the GTP node or nodes.                                                                                      |
| 6.                                                                                                                                        | <b>CPN</b> —Name of the CPN or CPNs.                                                                                             |
| 7.                                                                                                                                        | <b>UPN</b> —Name of the UPN or UPNs.                                                                                             |
| 8.                                                                                                                                        | <b>SAM</b> —Name of SAMs Exporter node or nodes.                                                                                 |
| 9.                                                                                                                                        | <b>Sites</b> —Name of the site or sites and the names of the CPN/UPN participating in the site or sites.                         |
| 10.                                                                                                                                       | <b>CUPS</b> —Name of the file containing information of the solution level RBAC Tags.                                            |

File name: mobility\_inventory (Single GigaVUE-FM instance)

```
[IPInterfaceSolution]
ip_interface_solution

[ToolGroups]
cluster-two
cluster-one

[Gigastreams]
cluster-two
cluster-one

[GTPWhitelist]
cluster-two
cluster-one

[Ports]
cluster-two
cluster-one

[Policies]
gtp_policy

[GTP]
gtp_1

[CPN]

[UPN]

[SAM]
sam1

[Sites]
UK gtp_list='["gtp1"]' upn_list='[]' sam_list='[sam1]'

[MobilitySolution]
mobilitySolution1 non_cups_lte_global_policy=gtp_policy sites='["UK"]'
```

File name: cups\_inventory (Multiple GigaVUE-FM instances)

```
[IPInterfaceSolution]
ip_interface_solution config
```

```

[ToolGroups]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[gigastreams]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[GTPWhitelist]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Ports]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Policies]
gtp_policy

[GTP]
gtp_1

[CPN]

[UPN]

[SAM]
sam1

[Sites]
UK gtp_list=["gtp1"] cpn_list=[] upn_list=[]
sam_list=["sam1"]
Dallas gtp_list=["gtp1"] cpn_list=[] upn_list=[]
sam_list=["sam1"]

[MobilitySolution]
mobilitySolution1 non cups lte global policy=gtp_policy sites=["UK"] fm_ip=192.168.36.2
mobilitySolution2 non cups lte global policy=gtp_policy sites=["Dallas"] fm_ip=192.168.36.3

```

## Creating host\_vars directory

Create **host\_vars** directory inside the Inventory Directory.

```
gigamon@fmreg26:~/CP-Metadata-Solution$ mkdir host_vars
```

```
gigamon@fmreg26:~/CP-Metadata-Solution$ ls -l
```

```
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
```

```
-rw-r--r-- 1 gigamon fmtaf 396 May 11 14:22 mobility_inventory
```

```
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

```
drwxr-xr-x 2 gigamon fmtaf 4096 May 11 14:48 host_vars
```

## Creating host\_vars files

Every unique element under each group in the **mobility\_inventory** file needs to have a file, with the same name as the element, inside **host\_vars** directory. This file has properties of the groups that it belongs to.

Following are the templates of various host\_vars files.

### Prerequisite

```

validate_certs: false
Ports:
- port:
 - 1/1/x1
 - 1/1/x2
adminStatus: enable
type: network

GTPWhitelist:
- alias: gtp1
imsi: 310260564627811,310260564627812
state: present
- alias: gtp2
inputFile: './whitelistKeys/TenIMSIIs_Valid.txt'
state: present

Gigastreams:
- alias: toolGS_C11
ports:
 - 4/1/x1
 - 4/1/x2
type: hybrid
state: present
- alias: toolGS_C12
ports:
 - 4/1/x3,x4
type: hybrid
state: present

ToolGroups:
- alias: pgGrp_C11
ports:
 - 2/1/x1
smartlb: false
type: tool
state: present
- alias: pgGrp_C12
ports:
 - 2/1/x2
smartlb: false
type: tool
```

state: present

## Site

For information about Site, refer to [Schema](#).

## cpNode

For information about cpNode, refer to [Schema](#).

## upNode

For information about upNode, refer to [Schema](#).

## 5GPolicy

For information about 5GPolicy, refer to [Schema](#).

## LTEPolicy

For information about LTEPolicy, refer to [Schema](#).

# Deployment of 3G/4G Control Plane Metadata Solution

To deploy the 3G/4G control plane metadata solution, follow these steps:

## Set up of additional variable for Single GigaVUE-FM instance

For a single GigaVUE-FM instance deployment, you must set an additional environment variable as follows.

```
export ANSIBLE_FM_IP=192.168.36.2
```

It searches the login details of the GigaVUE-FM IP in *fmInfo.yml* file.

## Execute the Playbook

You can execute the playbook and deploy the 3G/4G control plane metadata solution using the following command:

```
/usr/bin/ansible-playbook -e '@~/CP-Metadata-Solution/ansible_inputs.json' -i ~/CP-Metadata-Solution/mobility_inventory /usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_mobility_solution.yml
```

If the *fmInfo* file is encrypted, use the following command to execute and deploy 3G/4G control plane metadata solution:

```
/usr/bin/ansible-playbook -e '@~/CP-Metadata-Solution/ansible_inputs.json' -
-ask-vault-pass -i ~/CP-Metadata-Solution/mobility_inventory
/usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_
mobility_solution.yml
```

**NOTE:** The multiple YML files created inside the **host\_vars** are concatenated, converted into JSON format and sent to GigaVUE-FM.

### Configuration of 5G Control Plane Metadata using Ansible

To configure 5G control plane metadata, perform the following steps:

| S.No | Steps                               | Refer to..                                                        |
|------|-------------------------------------|-------------------------------------------------------------------|
| 1.   | Creating Inventory Directory        | <a href="#">Creating Inventory Directory</a>                      |
| 2.   | Creating <i>fmInfo.yml</i>          | <a href="#">Creating fmInfo.yml</a>                               |
| 3.   | Creating <i>ansible_inputs.json</i> | <a href="#">Creating ansible_inputs.json</a>                      |
| 4.   | Creating 5G inventory file          | <a href="#">Creating 5G control plane metadata inventory file</a> |
| 5.   | Creating <b>host_vars</b> directory | <a href="#">Creating host_vars directory</a>                      |
| 6.   | Creating <b>host_vars</b> files     | <a href="#">Creating host_vars files</a>                          |

## Creating Inventory Directory

Create an Inventory Directory to store all the 5G control plane metadata related configuration files.

```
username@fmreg26:~$ mkdir 5g-Metadata-Solution
username@fmreg26:~$ ls -l
drwxr-xr-x 2 daniel fmfaf 4096 May 11 11:59 5g-Metadata-Solution
```

## Creating fmInfo.yml

Create fmInfo.yml file inside the Inventory Directory that contains the information such as ip-address, username and password. To create the file, refer to [Schema](#).

## Creating ansible\_inputs.json

Create 'ansible\_inputs.json' file inside the Inventory Directory.

```
gigamon@fmreg26:~/5G-Metadata-Solution$ ls -l
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

File name: ansible\_inputs.json To create a file, refer to [Schema](#).

## Creating 5G control plane metadata inventory file

Create the **mobility\_inventory** file inside Inventory Directory.

```
gigamon@fmreg26:~/5g-Metadata-Solution$ touch mobility_inventory
```

```
gigamon@fmreg26:~/5g-Metadata-Solution$ ls -l
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
-rw-r--r-- 1 gigamon fmtaf 396 May 11 14:22 mobility_inventory
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

The file contains the details of the following groups and provide the inputs to the groups as shown in the following table:

| S.No                                                                                                                                      | Groups-Input                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Note:</b> –You can provide the input or leave the field empty if you don't want to use the playbook to configure the following groups. |                                                                                                                                  |
| 1.                                                                                                                                        | <b>Ports</b> —Name of the Cluster or standalone device IP that contains the ports that need to be configured.                    |
| 2.                                                                                                                                        | <b>IPInterfaceSolution</b> —Name of the Cluster or standalone device IP on which the IPInterfacesolution needs to be configured. |
| 3.                                                                                                                                        | <b>Tool Groups</b> —Name of the Cluster or standalone device IP on which the ToolGroup needs to be configured.                   |
| 4.                                                                                                                                        | <b>GigaStreams</b> —Name of the Cluster or standalone device IP on which the Gigastreams needs to be configured.                 |
| 5.                                                                                                                                        | <b>GTPWhitelist</b> —Name of the Cluster or standalone device IP on which the GTPWhitelist database needs to be configured.      |
| 6.                                                                                                                                        | <b>Policies</b> —Name of the Global policy or policies.                                                                          |
| 7.                                                                                                                                        | <b>GTP</b> — Name of the GTP node or nodes.                                                                                      |
| 6.                                                                                                                                        | <b>CPN</b> —Name of the CPN or CPNs.                                                                                             |
| 7.                                                                                                                                        | <b>UPN</b> —Name of the UPN or UPNs.                                                                                             |
| 8.                                                                                                                                        | <b>SAM</b> —Name of SAMs Exporter node or nodes.                                                                                 |
| 9.                                                                                                                                        | <b>Sites</b> —Name of the site or sites and the names of the CPN/UPN participating in the site or sites.                         |
| 10.                                                                                                                                       | <b>CUPS</b> —Name of the file containing information of the solution level RBAC Tags.                                            |

File name: mobility\_inventory (Single GigaVUE-FM instance)

```
[IPInterfaceSolution]
ip_interface_solution

[ToolGroups]
cluster-two
cluster-one

[Gigastreams]
cluster-two
cluster-one

[GTPWhitelist]
cluster-two
cluster-one

[Ports]
cluster-two
cluster-one

[Policies]
5g_policy_1

[GTP]

[CPN]
5g_cpn

[UPN]

[SAM]
sam1

[Sites]
UK cpn_list='["5g_cpn"]' upn_list='[]' sam_list='["sam1"]'

[MobilitySolution]
mobilitySolution1 cups_5g_global_policy=5g_policy_1 sites='["UK"]'
```

File name: cups\_inventory (Multiple GigaVUE-FM instances)

```
[IPInterfaceSolution]
ip_interface_solution_config
```

```

[ToolGroups]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Gigastreams]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[GTPWhitelist]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Ports]
cluster-two fm_ip=192.168.36.2
cluster-one fm_ip=192.168.36.3

[Policies]
5g_policy_1

[GTP]

[CPN]
5g_cpn

[UPN]

[SAM]
sam1

[Sites]
UK cpn_list='["5g_cpn"]' upn_list='[]' sam_list='[sam1]'
Dallas cpn_list='["5g_cpn"]' upn_list='[]' sam_list='[sam1]'

[MobilitySolution]
mobilitySolution1 cups_5g_global_policy=5g_policy_1 sites='["UK"]' fm_ip=192.168.36.2
mobilitySolution2 cups_5g_global_policy=5g_policy_1 sites='["Dallas"]' fm_ip=192.168.36.3

```

## Creating host\_vars directory

Create **host\_vars** directory inside the Inventory Directory.

```
gigamon@fmreg26:~/5g-Metadata-Solution$ mkdir host_vars
```

```
gigamon@fmreg26:~/5g-Metadata-Solution$ ls -l
```

```
-rw-r--r-- 1 gigamon fmtaf 355 May 11 12:24 ansible_inputs.json
```

```
-rw-r--r-- 1 gigamon fmtaf 396 May 11 14:22 mobility_inventory
```

```
-rw-r--r-- 1 gigamon fmtaf 172 May 11 12:10 fmInfo.yml
```

```
drwxr-xr-x 2 gigamon fmtaf 4096 May 11 14:48 host_vars
```

## Creating host\_vars files

Every unique element under each group in the **mobility\_inventory** file needs to have a file, with the same name as the element, inside **host\_vars** directory. This file has properties of the groups that it belongs to.

Following are the templates of various host\_vars files.

### Prerequisite

```

validate_certs: false
Ports:
- port:
 - 1/1/x1
 - 1/1/x2
adminStatus: enable
type: network

GTPWhitelist:
- alias: gtp1
 imsi: 310260564627811,310260564627812
 state: present
- alias: gtp2
 inputFile: './whitelistKeys/TenIMSIIs_Valid.txt'
 state: present

Gigastreams:
- alias: toolGS_C11
 ports:
 - 4/1/x1
 - 4/1/x2
 type: hybrid
 state: present
- alias: toolGS_C12
 ports:
 - 4/1/x3,x4
 type: hybrid
 state: present

ToolGroups:
- alias: pgGrp_C11
 ports:
 - 2/1/x1
 smartlb: false
 type: tool
 state: present
- alias: pgGrp_C12
 ports:
 - 2/1/x2
 smartlb: false
 type: tool
```

state: present

## Site

For information about Site, refer to [Schema](#).

## cpNode

For information about cpNode, refer to [Schema](#).

## upNode

For information about upNode, refer to [Schema](#).

## 5GPolicy

For information about 5GPolicy, refer to [Schema](#).

## LTEPolicy

For information about LTEPolicy, refer to [Schema](#).

# Deployment of 3G/4G Control Plane Metadata Solution

To deploy the 3G/4G control plane metadata solution, follow these steps:

## Set up of additional variable for Single GigaVUE-FM instance

For a single GigaVUE-FM instance deployment, you must set an additional environment variable as follows.

```
export ANSIBLE_FM_IP=192.168.36.2
```

It searches the login details of the GigaVUE-FM IP in *fmInfo.yml* file.

## Execute the Playbook

You can execute the playbook and deploy the 5G control plane metadata solution using the following command:

```
/usr/bin/ansible-playbook -e '@~/5g-Metadata-Solution/ansible_inputs.json' -i ~/5g-Metadata-Solution/mobility_inventory /usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_mobility_solution.yml
```

If the *fmInfo* file is encrypted, use the following command to execute and deploy 5G control plane metadata solution:

```
/usr/bin/ansible-playbook -e '@~/5g-Metadata-Solution/ansible_inputs.json' -
-ask-vault-pass -i ~/5g-Metadata-Solution/mobility_inventory
/usr/local/share/gigamon-ansible/playbooks/mobility_solution/deploy_
mobility_solution.yml
```

**NOTE:** The multiple YML files created inside the **host\_vars** are concatenated, converted into JSON format and sent to GigaVUE-FM.

## CPN-UPN Communication for Support of RAN and Network Slice Attributes

CPN-UPN Communication enables traffic management based on Radio Access Network (RAN) and Network Slice attributes in the Standalone User Plane Node (UPN). This feature allows you to enable flow sampling and forward listing based on the RAN attributes and flow sampling based on the Network Slice attributes. This is achieved by establishing communication between Control Plane Node and the Standalone UPN.

The CUPS architecture provides network visibility across the control and user planes for the 5G standalone packet core network. The UPN processes the GTP-u traffic using the subscriber correlation from the control plane PFCP protocols available at the user plane sites. UPN enriches the subscriber information extracted from the Gigamon PFCP message (GPFCP) packets received from CPN for enhanced flow sampling and forward listing capabilities.

By establishing a communication between CPN and UPN, the RAN and the Network Slice Attributes from the CPN are exchanged with UPN, which allows UPN to flow sample and forward list the traffic based on the RAN attributes and flow sample the traffic based on Network Slice attributes.

The CPN-UPN Communication solution includes the following components:

- CPN: can be 4G or 5G
- Standalone UPN

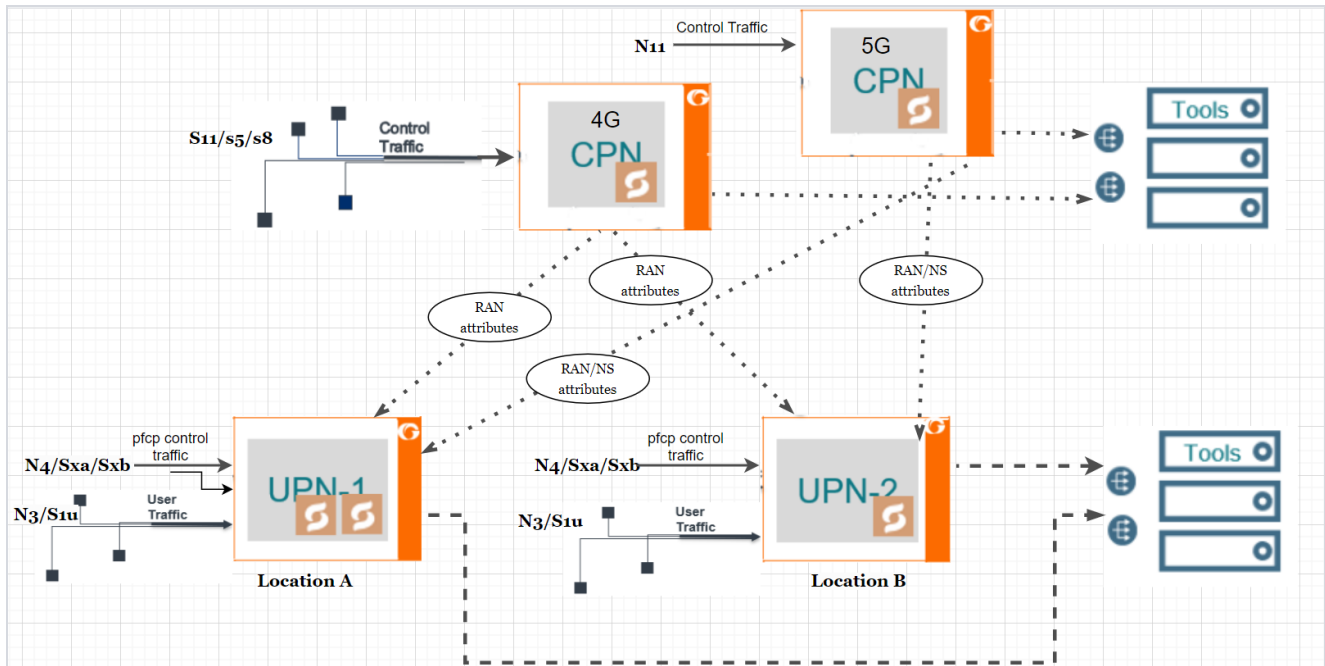
UPN supports the following parameters based on the attributes received from CPN:

### RAN flow sampling and forward listing parameters

- E-UTRAN Cell Global Identifier (ECGI) (MCC+MNC+ECI)
- New Radio Cell Global Identifier (NCGI) (MCC+MNC+NCI)
- Tracking Area Code (TAC)
- Tracking Area Identity (TAI) (MCC+MNC+TAC)

### Network Slice flow sampling parameters

- S-NSSAI with standardized SST (Slice/Service Type)
- S-NSSAI non-standard SST values with and without SD



The above topology explains how CPN and UPN communicate with each other.

In the above topology, the 4G CPN receives control traffic from the S11/S5/S8 interface, while the 5G CPN receives control traffic from the N11 interface. UPN-1 and UPN-2 receive PCF traffic from the N4/Sxa/Sxb interface. Upon receiving PCF traffic, UPN generates a session table that does not include the RAN and Network Slice Attributes.

The communication between CPN and UPN is facilitated using the GPFPCP. GPFPCP messages are never fragmented, and the message exchange between CPN and UPN is always less than 1500 bytes. Once the communication is established using GPFPCP, the CPN pushes the RAN and Network Slice attributes to the UPN based on a request and appends the session table with the RAN and Network Slice attributes. In case of failures, UPN can also request the RAN and Network Slice attributes from CPN.

Once the UPN receives the user traffic from N3/S1u interface, based on the map rules configured in the UPN, the correlation takes place. With the RAN and Network Slice (NS) attributes from the CPN, the UPN now has the ability to flow sample and forward list the traffic based on the RAN and Network Slice Attributes. RAN and Network Slice information is not added to the packets sent out by UPN.

Keep in mind the following when configuring CPN-UPN Communication solution:

- UPN will back up and restore the sessions with the session attributes received from CPN.
- 4G CPN supports only RAN Attributes.
- The GPFPCP messages are exchanged through UDP and are not encrypted.
- The UDP port used for the CPN-UPN communication must be within the ephemeral range (49152 to 65535).
- The GPFPCP messages are not fragmented.

To know more about CPN-UPN communication configuration, communication statistics, map rules, upgrade, and rollback, refer to the following sections:

- [CPN-UPN Communication Configuration](#)
- [View CUPS Communication Dashboard](#)
- [Map Rules for CPN-UPN Communications](#)
- [Upgrade Standalone UPN to CPN-UPN Communication Solution](#)
- [Rollback from CPN-UPN Communication Solution to Standalone UPN](#)
- [Quick Rollback from CPN-UPN Communication Solution to Standalone UPN](#)

### CPN-UPN Communication Configuration

CPN-UPN Communication can be configured in either of the following two ways. Refer to the following sections for step-by-step instructions:

- [Configure CPN-UPN Communication using Ansible](#)
- [Configure CPN-UPN Communication using CLI](#)

## Configure CPN-UPN Communication using Ansible

To configure CPN-UPN Communication using Ansible:

| Step No | Task                                                                                          | Refer to the following topics                                                                    |
|---------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 1.      | Configure CPN                                                                                 | <a href="#">GigaSMART 5G CUPS</a>                                                                |
| 2.      | Configure UPN                                                                                 | <a href="#">PCFP Messages</a>                                                                    |
| 3.      | Install Gigamon Ansible Module                                                                | <a href="#">Installation and Configuration of Subscriber Intelligence Solution using Ansible</a> |
| 4.      | Create Inventory Directory to store all the CPN-UPN Communication related configuration files | <a href="#">Create Inventory Directory</a>                                                       |
| 5.      | Create <b>fmInfo.yml</b> for Ansible to access GigaVUE-FM, GigaVUE HC Series                  | <a href="#">Create fmInfo.yml</a>                                                                |
| 6.      | Create <b>ansible_inputs.json</b>                                                             | <a href="#">Create ansible_inputs.json File</a>                                                  |
| 7.      | Create CPN-UPN Communication inventory file                                                   | <a href="#">Create an Inventory File for CPN UPN Communication</a>                               |
| 8.      | Create <b>host_vars</b> directory                                                             | <a href="#">Create host_vars directory</a>                                                       |
| 9.      | Create <b>host_vars</b> files                                                                 | <a href="#">Create host_vars files</a>                                                           |
| 10.     | Deploy CPN-UPN Communication solution in Ansible                                              | <a href="#">Deploy CPN-UPN Communication Solution in Ansible</a>                                 |
| 11.     | View the configured CPN-UPN Communication solution in GigaVUE-FM, GigaVUE HC Series           | <a href="#">View CPN-UPN Communication Solution in GigaVUE-FM, GigaVUE HC Series</a>             |
| 12.     | View Dashboard                                                                                | <a href="#">View CUPS Communication Dashboard</a>                                                |

## Configure CPN-UPN Communication using CLI

| Step No                                                                                                                           | Task                                                           | Refer to the following topics                                      |
|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|--------------------------------------------------------------------|
| 1                                                                                                                                 | Configure ports                                                | <a href="#">ports</a>                                              |
| 2                                                                                                                                 | Configure GigaStream                                           | <a href="#">gigastream</a>                                         |
| 3                                                                                                                                 | Create GPFCP profile                                           | <a href="#">gpfcf profile</a>                                      |
| 4                                                                                                                                 | Configure UPN Interface profile                                | <a href="#">Configure Custom Interface Selection</a>               |
| 5                                                                                                                                 | Configure GigaSMART group                                      | <a href="#">gsgroups</a>                                           |
| 6                                                                                                                                 | Configure IP interface                                         | <a href="#">ip interface</a>                                       |
| 7                                                                                                                                 | Configure the exporter                                         | <a href="#">apps exporter</a>                                      |
| 8                                                                                                                                 | Define the node role                                           | <a href="#">gsparams</a>                                           |
| 9                                                                                                                                 | Create GigaSMART operations                                    | <a href="#">gsop</a>                                               |
| 10                                                                                                                                | Create a Vport                                                 | <a href="#">vport</a>                                              |
| 11                                                                                                                                | Define first level map to send the traffic to Vport            | <a href="#">map</a>                                                |
| 12                                                                                                                                | Create a second level map with flow sample/ forward list rules | <a href="#">map</a>                                                |
| The following configuration example explains the entire configuration flow for 4G CPN (when one 4G CPN communicates with one UPN) |                                                                |                                                                    |
| CPN-UPN Communication configuration example                                                                                       |                                                                | <a href="#">Configure CPN-UPN Communication solution using CLI</a> |

### Configure CPN-UPN Communication Solution using Ansible

To configure CPN-UPN Communication using Ansible:

- [Create Inventory Directory](#)
- [Create fmInfo.yml](#)
- [Create ansible\\_inputs.json File](#)
- [Create an Inventory File for CPN-UPN Communication](#)
- [Create host\\_vars directory](#)
- [Create host\\_vars files](#)
- [Create host\\_vars files](#)
- [Deploy CPN-UPN Communication Solution in Ansible](#)
- [View CPN-UPN Communication Solution in GigaVUE-FM, GigaVUE HC Series](#)

## Create Inventory Directory

Create an *Inventory Directory* to store all the CPN-UPN Communication related configuration files.

```
username@fmreg26:~$ mkdir cupsSolution
```

## Create *fmInfo.yml*

Create *fmInfo.yml* file inside the inventory directory with the IP address, username, and password of GigaVUE-FM. This helps Ansible to fetch the details of GigaVUE-FM, GigaVUE HC Series.

## Create *ansible\_inputs.json* File

Create a json file *ansible\_inputs.json* inside the inventory directory that contains the path of the below mentioned files. This allows Ansible to identify and access the below mentioned files.

- *fm\_credential\_file* - Provide the path of the *fmInfo.yml* file.
- *yaml\_payload\_path* - Created automatically while running the cups playbook. Provide the path of the file that stores the payload sent to GigaVUE-FM.
- *golden\_payload\_path* - The payload of a successful cups solution deployment is saved in this file. Provide the file path that has the golden payload.
- *deployment\_report\_path* - Created automatically while running the cups playbook. This file stores the report of the deployment. Provide the path of the file.

## Create an Inventory File for CPN-UPN Communication

Create *mobility\_inventory* file inside the inventory directory.

Enter the details in the file as shown in the below example:

```
[IPInterfaceSolution]
<Name of the Cluster or standalone device IP that contains the ports that need to be
configured.>

[ToolGroups]
<Name of the Cluster or standalone device IP on which the Tool Group needs to be configured.>
<Name of the Cluster or standalone device IP on which the Tool Group needs to be configured.>

[Gigastreams]
<Name of the Cluster or standalone device IP on which the Gigastreams needs to be configured.>

[GTPWhitelist]
<Name of the Cluster or standalone device IP on which the GTPWhitelist Data Base needs to be
configured.>
```

```
[Ports]
<Name of the Cluster or standalone device IP that contains the ports that need to be
configured.>

[Policies]
<Name of the Global policy or policies.>

[CPN]
<Name of the CPN or CPNs.>

[UPN]
<Name of the CPN or CPNs.>

[Sites]
Site_Name1='["<Name of the CPN"""]' upn_list='[]' sam_list='[]'
Site_Name2='[]' upn_list='["Name of the UPN"]' sam_list='[]'

[MobilitySolution]
<Name of the file CPN UPN Communication solution along with lts_policy file name, 5g_policy
file name, lte_policy file name and list of sites participating in the CPN UPN Communication
solution.>
```

## Create **host\_vars** directory

Create **host\_vars** directory inside the inventory directory to host the files that are used in the ***mobility\_inventory*** file.

```
gigamon@fmreg26:~/cupsSolution$ mkdir host_vars
```

## Create **host\_vars** files

Each unique element like Ports, GigaStream, GTP forward list, and Tool Groups in the ***mobility\_inventory*** file needs to have a file, with the same name as the element, inside **host\_vars** directory.

For Example

- The element of name 'cpnUkLTE' under group 'CPN' has a file with name 'cpnUkLTE' inside host\_vars directory. This file has the properties of the CPN.
- The element of name 'cluster-one' has a file with name 'cluster-one' inside host\_vars directory. This has the properties of all the groups like Ports, IPInterface, ToolGroups, etc that the element is a member.

Below are a sample of a host\_vars files.

**Prerequisite:**

```

validate_certs: false
Ports:
- port:
 - 1/1/x1
 - 1/1/x2
 adminStatus: enable
 type: network

GTPWhitelist:
- alias: gtp1
 imsi: 310260564627811,310260564627812
 state: present
- alias: gtp2
 inputFile: './whitelistKeys/TenIMSIValid.txt'
 state: present

Gigastreams:
- alias: toolGS_C11
 ports:
 - 4/1/x1
 - 4/1/x2
 type: hybrid
 state: present
- alias: toolGS_C12
 ports:
 - 4/1/x3..x4
 type: hybrid
 state: present

ToolGroups:
- alias: pgGrp_C11
 ports:
 - 2/1/x1
 smartLb: false
 type: tool
 state: present
- alias: pgGrp_C12
 ports:
 - 2/1/x2
 smartLb: false
 type: tool
 state: present
```

## Site

Mobility Solutions are generally spread across multiple geographically dispersed data centers called sites.

A site is a collection of the following:

- Network element functions.
- Traffic access points for interfaces of such network element functions.
- Visibility and Analytics Fabric (VAF) nodes.

- Traffic monitoring or analysis tool devices (called probes) that are locally connected without using any IP routed tunnels.

```

Site:
 # Name of the site
 alias: UK
 # 'skipDeployment' attribute is 'false' for the sites that are intended to be deployed in the
 incremental deployment process
 skipDeployment: true
 # Tag values assigned to the site
 tags:
 - tagKey: Location
 tagValues:
 - UK
 # All the tools used in the site
 toolBindings:
 - alias: GeoProbe
 toolResourceType: GIGASTREAM
 toolClusterId: cluster-one
 toolResourceId: toolGS_C11
 - alias: EEA
 toolResourceType: PORTGROUP
 toolClusterId: cluster-one
 toolResourceId: pgGrp_C11
 # Network Ports. Fill as needed in the format 'clusterid:portId'
 networkPorts: []
 # Policies under 'siteOverrideOfPolicyArrangements' override global policies
 siteOverrideOfPolicyArrangements:
 forLTE:
 _file: /home/ddaniel/automationInventoryDirectory/host_vars/lte_policy_1.yml
 for5G: {}
 # Leave upNodes and cpNodes as empty
 upNodes: []
 cpNodes: []
```

## cpNode

```
--
ProcessingNode:
 # Name of the control processing node
 alias: cpnUKLTE
 # Tags assigned to the processing node
 tags:
 - tagKey: Dept
 tagValues:
 - IT
 - Engg
 # Type of control node. Possible values for the nodeType are: 'PCPN_LTE', 'PUPN', 'PCPN_5G'
 nodeType: PCPN_5G
 # Location of the gigasmart engine port assigned to the processing node
 location:
 clusterId: cluster-one
 enginePorts:
 - 2/3/e1
```

```
IP interface that needs to be used by the processing node
ipInterfaceAlias: dev3_IpIntUpn_1
gtpControlSample: false
gtpRandomSampling:
 enabled: false
 # min: 12, max: 48, multiples of 12hrs
 interval: 12
numberOfLteSessions: 100000
numberOf5gSessions: 100000
GS Group HTTP2 port list
app5gHTTP2Ports:
- 8080
- 9000
Network Ports. Fill as needed in the format 'clusterid:portId'
nodeOverrideNetworkPorts: []
trafficSources:
- networkFunctionName: cpn_pod1_SGW-C
 networkFunctionType: SGW-C
 tags:
 - tagKey: Dept
 tagValues:
 - IT
 - Engg
 networkFunctionInterfaces:
 - tunnelIdentifiers:
 - interfaceTunnelIdentifierType: IPADDRESS
 value: 255.255.255.0
 netMask: 198.51.100.42
 - interfaceTunnelIdentifierType: PORT
 value: 8805
 interfaceType: Sxa
 # Network Ports. Fill as needed in the format 'clusterid:portId'
 sourceOverrideNetworkPorts:
 - 192.168.65.8:8/1/x3
#TCP loadbalancing properties applicable only for nodeType PCPN_5G
appTcp:
 # Possible values for application are : 'broadcast', 'enhanced', 'drop'
 application: broadcast
 # Possible values for tcpControl are : 'broadcast', 'enhanced', 'drop'
 tcpControl: broadcast
 # To enable loadbalancing set value as true
 loadBalance: false
```

## upNode

```

ProcessingNode:
 # Name of the control processing node
 alias: upnDallas
 # Tags assigned to the processing node
 tags:
 - tagKey: Dept
 tagValues:
 - IT
 - Engg
```

```

Type of user node. Possible values for the nodeType are: 'PCPN_LTE', 'PUPN', 'PCPN_5G'
nodeType: PUPN
To make user node as standalone
standAloneMode: true
Location of the gigasmart engine port assigned to the processing node
location:
 clusterId: cluster-two
 enginePorts:
 - 6/3/e1
 - 6/3/e2
IP interface that needs to be used by the processing node
ipInterfaceAlias: dev3_IpIntUpn_1
gtpControlSample: false
gtpRandomSampling:
 enabled: false
 # min: 12, max: 48, multiples of 12hrs
 interval: 12
Network Ports. Fill as needed in the format 'clusterid:portId'
nodeOverrideNetworkPorts: []
trafficSources:
- networkFunctionName: upn_pod1_SGW-U
 networkFunctionType: SGW-U
 tags:
 - tagKey: Dept
 tagValues:
 - IT
 - Engg
 networkFunctionInterfaces:
 - tunnelIdentifiers:
 - interfaceTunnelIdentifierType: IPADDRESS
 mask: 255.255.255.0
 address: 198.58.100.45
 - interfaceTunnelIdentifierType: PORT
 value: 8805
 interfaceType: Sxa
 # Network Ports. Fill as needed in the format 'clusterid:portId'
 sourceOverrideNetworkPorts:
 - 192.168.65.9:9/1/x4
 - 192.168.65.9:9/1/x5
- networkFunctionName: upn_pod2_UPF
 networkFunctionType: UPF
 tags:
 - tagKey: Dept
 tagValues:
 - IT
 - Engg
 networkFunctionInterfaces:
 - tunnelIdentifiers:
 - interfaceTunnelIdentifierValue:
 mask: 255.255.255.0
 address: 198.58.100.46
 interfaceTunnelIdentifierType: IPADDRESS
 - interfaceTunnelIdentifierValue:
 value: '2152'
 interfaceTunnelIdentifierType: PORT
 interfaceType: N11
 sourceOverrideNetworkPorts:
 - 192.168.65.9:9/1/x6

```

## 5GPolicy

```

5GPolicy:
 # gtpFlowTimeout is multiplied by 10 minutes to arrive at a timeout interval.
 (gtpFlowTimeout: 48 = 8 hours). Set this interval to match customer network's GTP session
 timeout for optimal results
 gtpFlowTimeout: 48
 # gtpPersistence -- save state tables during reboot or box failure. Remove if not using
 persistence
 gtpPersistence:
 # interval in minutes to save state table (min value is 10)
 interval: 10
 restartAgeTime: 30
 fileAgeTimeout: 30
 sampling:
 flowMaps:
 - alias : samplingMap2
 rules:
 - interface:
 dnn: internet.miracle
 pei: '*'
 supi: 46*
 gpsi:
 nas_5qi:
 tac:
 nci:
 plmndId:
 nsiid:
 # -- "controlPlanePercentage: specifies percentage of sampling at CPN (set to 100 for
 no CPN sampling)
 controlPlanePercentage: 100
 # -- userPlanePercentage: specifies percentage of sampling at UPN (will be applied to
 all UPNs -- use site override to set different rates per site)
 userPlanePercentage: 50
 tool: EEA
 whitelisting:
 whiteListAlias: gtp1
 flowMaps:
 - alias : whitelistMap2
 rules:
 - dnn: internet.miracle
 interface:
 supi:
 ran:
 tool: EEA
 loadBalancing:
 # one of { flow5g }
 appType: flow5g
 # metric is the load balancing method -- one of { leastBw, leastPktRate, leastConn,
 leastTotalTraffic, roundRobin, wtLeastBw, wtLeastPktRate, wtLeastConn, wtLeastTotalTraffic,
 wtRoundRobin, flow5gKeyHash}
 metric: flow5gKeyHash
 # hashingKey -- ignored if metric is not of type 'flow5gKeyHash' -- one of { supi | pei |
 gpsi }
 hashingKey: supi

```

## LTEPolicy

```

LTEPolicy:
 # gtpFlowTimeout is multiplied by 10 minutes to arrive at a timeout interval.
 (gtpFlowTimeout: 48 = 8 hours). Set this interval to match customer network's GTP session
 timeout for optimal results
 gtpFlowTimeout: 48
 # gtpPersistence -- save state tables during reboot or box failure. Remove if not using
 persistence
 gtpPersistence:
 # interval in minutes to save state table (min value is 10)
 interval: 10
 restartAgeTime: 30
 fileAgeTimeout: 30
 sampling:
 flowMaps:
 - alias : samplingMap1
 rules:
 - interface:
 version: any
 apn: internet.miracle
 imei: 123*
 imsi:
 msisdn:
 qci:
 # -- controlPlanePercentage: specifies percentage of sampling at CPN (set to 100 for no
 CPN sampling)
 controlPlanePercentage: 100
 # -- userPlanePercentage: specifies percentage of sampling at UPN (will be applied to
 all UPNs -- use site override to set different rates per site)
 userPlanePercentage: 50
 tool: GeoProbe
 whitelisting:
 whiteListAlias: gtp1
 flowMaps:
 - alias : whitelistMap1
 rules:
 - version: v1
 interface:
 apn:
 tool: GeoProbe
 loadBalancing:
 # one of { gtp | aft | tunnel }
 appType: gtp
 # metric is the load balancing method -- one of # { leastBw, leastPktRate, leastConn,
 leastTotalTraffic, roundRobin, wtLeastBw, wtLeastPktRate, wtLeastConn, wtLeastTotalTraffic,
 wtRoundRobin, gtpKeyHash}
 metric: gtpKeyHash
 # hashingKey -- ignored if metric is not of type 'gtpKeyHash' -- one of { imsi | imei |
 msisdn }
 hashingKey: imsi

```

## Deploy CPN-UPN Communication Solution in Ansible

To deploy the CPN-UPN Communication solution, follow these steps:

1. Set an additional environment variable to search the login details of the GigaVUE-FM IP in *fmlInfo.yml* file as follows.

```
export ANSIBLE_FM_IP=<GigaVUE-FM IP Address>
```

2. Execute the playbook and deploy the CPN-UPN Communication solution using the following command:

- If *fmlInfo.yml* file is not encrypted, use the following command:

```
/usr/bin/ansible-playbook -e '@~/cupsSolution/ansible_inputs.json' -i
~/cupsSolution/cups_inventory /usr/local/share/gigamon-
ansible/playbooks/cups/deploy_cups.yml
```

- If *fmlInfo.yml* file is encrypted, use the following command:

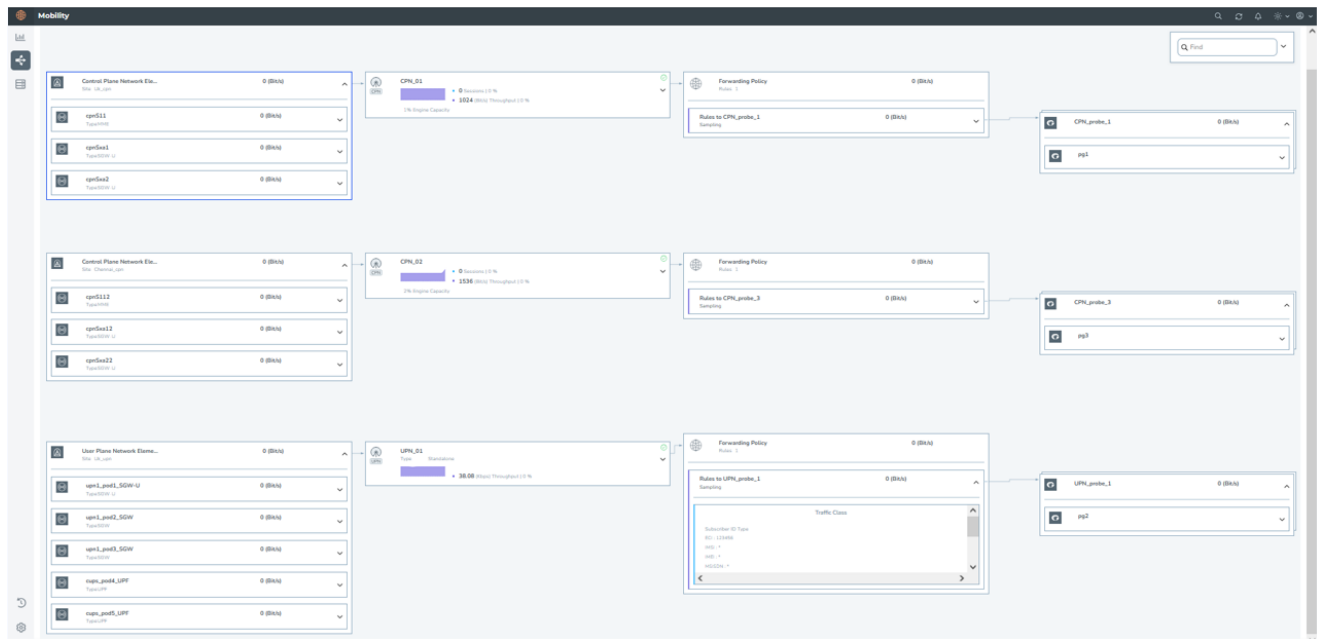
```
/usr/bin/ansible-playbook -e '@~/cupsSolution/ansible_inputs.json' -i
~/cupsSolution/cups_inventory /usr/local/share/gigamon-
ansible/playbooks/cups/deploy_cups.yml
```

## View CPN-UPN Communication Solution in GigaVUE-FM,GigaVUE HC Series

After deploying the CPN-UPN Communication in Ansible, you can view how the communication is established between CPN and UPN in GigaVUE-FM,GigaVUE HC Series. Follow the steps given below:

1. In GigaVUE-FM,GigaVUE HC Series, go to **Traffic > Physical > Orchestrated Flows**.
2. Click **Mobility**.
3. Click the **Alias**.

The following image shows the CPN-UPN communication solution:



After configuring CPN-UPN Communication solution, you can view the analytics and statistics in the CUPS Communication dashboard. Refer to [View CUPS Communication Dashboard](#) for more detailed information.

## Remove CPN-UPN Communication

To remove the CPN-UPN Communication solution, follow these steps:

- Execute the playbook and use the following command:  

```
/usr/local/bin/ansible-playbook -e '@~/<Path to Inventory directory>/ansible_inputs.json' -i ~/<Path to Inventory directory>/mobility_inventory /<Path to Ansible playbook>/delete_mobility_solution.yml
```

**NOTE:** The multiple YML files created inside the **host\_vars** are concatenated, converted into JSON format and sent to GigaVUE-FM.

### Map Rules for CPN-UPN Communication

The following tables explain the behavior of PFCP and GTP-u packets on UPN node when Flow sample and Forward list maps are configured with different combination of attributes.

## Flow Sample Map Rules for CPN-UPN Communication

### Rules and Notes:

- For PFCP packets, RAN and Network Slice based flow sampling are not applicable as the PFCP packets do not contain any RAN or Network Slice parameters.

- For GTP-u packets, if RAN and Network Slice enrichment are not performed, the packets will trigger a RAN PULL to get RAN information from the CPN. During this process (~3 seconds), GTP-u packets will be evaluated against any configured rules. If no match is found, they will either be dropped or sent to the collector. After this (~3 seconds), RAN or Network Slice flow sampling will apply if RAN enrichment is successful. If enrichment fails, GTP-u packets will again be evaluated against matching rules, dropped, or sent to the collector.
- Below are the list of generic RAN, non RAN, and Network Slice parameters that can be configured for CPN-UPN communication:
  - **Generic filter parameters** - apn/imsi/imei/msisdn/version/interface
  - **RAN filter parameters** - eci/plmn-id/tac/tac-5g/nci
  - **Network Slice parameters** - nssid [SST or SST.SD] SD is optional

| Generic Filter Parameters | RAN Filter Parameters | Network Slice Parameters | Flow sampling Status - PFCP Packets                                                                                                                                                        | Flow sampling Status - GTP-u packets                                                                                                                                                                                       |
|---------------------------|-----------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Yes                       | No                    | No                       | <ul style="list-style-type: none"> <li>PFCP packets matching the <b>Generic Filter</b> parameters configured are only flow sampled</li> <li>RAN flow sampling is not applicable</li> </ul> | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>Generic Filter</b> parameters configured are only flow sampled</li> <li>RAN and Network Slice based flow sampling is not considered</li> </ul>        |
| No                        | Yes                   | No                       | <ul style="list-style-type: none"> <li>All PFCP packets are flow sampled</li> <li>RAN flow sampling is not applicable</li> </ul>                                                           | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>RAN Filter</b> parameters configured are only flow sampled</li> <li>Network Slice based flow sampling is not considered</li> </ul>                    |
| Yes                       | Yes                   | No                       | <ul style="list-style-type: none"> <li>PFCP packets matching the <b>Generic Filter</b> parameters configured are only flow sampled</li> <li>RAN flow sampling is not applicable</li> </ul> | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>RAN Filter and Generic Filter</b> parameters configured are only flow sampled</li> <li>Network Slice based flow sampling is not considered</li> </ul> |
| No                        | No                    | Yes                      | <ul style="list-style-type: none"> <li>All PFCP packets are flow sampled</li> <li>RAN and Network Slice flow sampling is not applicable</li> </ul>                                         | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>Network Slice</b> parameters are only flow sampled</li> <li>RAN based flow sampling is not considered</li> </ul>                                      |
| No                        | Yes                   | Yes                      | <ul style="list-style-type: none"> <li>All PFCP packets are flow sampled</li> </ul>                                                                                                        | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>RAN and Network Slice</b> parameters are</li> </ul>                                                                                                   |

| Generic Filter Parameters | RAN Filter Parameters | Network Slice Parameters | Flow sampling Status - PFCP Packets                                                                                                                                                                          | Flow sampling Status - GTP-u packets                                                                                                                                                                     |
|---------------------------|-----------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           |                       |                          | <ul style="list-style-type: none"> <li>RAN and Network Slice flow sampling is not applicable</li> </ul>                                                                                                      | only flow sampled                                                                                                                                                                                        |
| Yes                       | No                    | Yes                      | <ul style="list-style-type: none"> <li>PFCP packets matching the <b>Generic Filter</b> parameters configured are only flow sampled</li> <li>RAN and Network Slice flow sampling is not applicable</li> </ul> | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>Generic Filter and Network Slice</b> parameters are only flow sampled</li> <li>RAN based flow sampling is not considered</li> </ul> |
| Yes                       | Yes                   | Yes                      | <ul style="list-style-type: none"> <li>PFCP packets matching the <b>Generic Filter</b> parameters configured are only flow sampled</li> <li>RAN and Network Slice flow sampling is not applicable</li> </ul> | <ul style="list-style-type: none"> <li>GTP-u packets matching the <b>Generic Filter, RAN and Network Slice</b> parameters are only flow sampled</li> </ul>                                               |

**NOTE:** In UPN, when the flow sampling map contains both RAN related and generic rules, the session count in the map statistics increments when both types of rules are matched. This behaviour is expected, as the rule lookup occurs twice: before and after enrichment. The initial rule lookup takes place when user tunnels are created from the PFCP packet, incrementing the session count for generic matching rules. After enrichment, a RAN update from the CPN triggers a second rule lookup to match RAN rules. For 5G sessions, the session count is based on the QFI per PDU session after enrichment.

## Forward List Map Rules for CPN-UPN Communication

### Rules and Notes:

- For PFCP packets filtered for matching, RAN forward list is Not Applicable as the PFCP packets do not contain any RAN parameters.
- For GTP-u packets filtered for matching, if RAN enrichment is not performed, the packets will trigger a RAN PULL to get RAN information from the CPN. During this process (~3 seconds), GTP-u packets will be evaluated against any configured rules. If no match is found, they will either be dropped or sent to the collector. After this (~3 seconds), RAN filtering will work if RAN enrichment is successful. If enrichment fails, GTP-u packets will again be evaluated against matching rules, dropped, or sent to the collector.

| Database Contains | Forward list Type | Forward list Rule - APN | Forward list Rule - Interface | PFCP Packets Filtered for Matching                                                                                                                                                                     | GTP-U Packets Filtered Matching                                                                                                                                                                         |
|-------------------|-------------------|-------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IMSI + RAN        | IMSI              | Yes                     | Yes                           | <b>IMSI + APN + Interface</b> <ul style="list-style-type: none"> <li>• PFCP packets matching IMSI, APN, and Interface are only forward listed</li> <li>• RAN forward list is not applicable</li> </ul> | <b>IMSI + APN + Interface</b> <ul style="list-style-type: none"> <li>• GTP-u packets matching IMSI, APN, and Interface are only forward listed</li> <li>• RAN forward list is not considered</li> </ul> |
| IMSI + RAN        | IMSI              | No                      | Yes                           | <b>IMSI + Interface</b> <ul style="list-style-type: none"> <li>• PFCP packets matching IMSI and Interface are only forward listed</li> <li>• RAN forward list is not applicable</li> </ul>             | <b>IMSI + Interface</b> <ul style="list-style-type: none"> <li>• GTP-u packets matching IMSI and Interface are only forward listed</li> <li>• RAN forward list is not considered</li> </ul>             |
| IMSI + RAN        | IMSI              | Yes                     | No                            | <b>IMSI + APN</b> <ul style="list-style-type: none"> <li>• PFCP packets matching IMSI and APN are only forward listed</li> <li>• RAN forward list is not applicable</li> </ul>                         | <b>IMSI + APN</b> <ul style="list-style-type: none"> <li>• GTP-u packets matching IMSI and APN are only forward listed</li> <li>• RAN forward list is not considered</li> </ul>                         |
| IMSI + RAN        | IMSI              | No                      | No                            | <b>IMSI</b> <ul style="list-style-type: none"> <li>• PFCP packets matching IMSI are forward listed</li> <li>• RAN forward list is not applicable</li> </ul>                                            | <b>IMSI</b> <ul style="list-style-type: none"> <li>• GTP-u packets matching IMSI are only forward listed</li> <li>• RAN forward list is not considered</li> </ul>                                       |
| IMSI + RAN        | RAN               | Yes                     | Yes                           | <b>APN + Interface</b> <ul style="list-style-type: none"> <li>• PFCP packets matching APN and Interface are only forward listed</li> <li>• RAN forward list is not applicable</li> </ul>               | <b>RAN + APN + Interface</b> <ul style="list-style-type: none"> <li>• GTP-u packets matching the RAN, APN, and Interface are only forward listed</li> </ul>                                             |
| IMSI + RAN        | RAN               | No                      | Yes                           | <b>Interface</b> <ul style="list-style-type: none"> <li>• PFCP packets matching the Interface are only forward listed</li> <li>• RAN forward list is not applicable</li> </ul>                         | <b>RAN + Interface</b> <ul style="list-style-type: none"> <li>• GTP-u packets matching the RAN and Interface are only forward listed</li> </ul>                                                         |

| Database Contains | Forward list Type | Forward list Rule - APN | Forward list Rule - Interface | PFCP Packets Filtered for Matching                                                                                                                                                                 | GTP-U Packets Filtered Matching                                                                                                                                    |
|-------------------|-------------------|-------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IMSI + RAN        | RAN               | Yes                     | No                            | <b>APN</b> <ul style="list-style-type: none"> <li>PFCP packets matching APN are only forward listed</li> <li>RAN forward list is not applicable</li> </ul>                                         | <b>RAN + APN</b> <ul style="list-style-type: none"> <li>GTP-u packets matching RAN and APN are only forward listed</li> </ul>                                      |
| IMSI + RAN        | RAN               | No                      | No                            | <b>All PASS</b> <ul style="list-style-type: none"> <li>All PFCP packets are forward listed</li> <li>RAN forward list is not applicable</li> </ul>                                                  | <b>RAN</b> <ul style="list-style-type: none"> <li>GTP-u packets matching the RAN are only forward listed</li> </ul>                                                |
| IMSI + RAN        | ALL               | Yes                     | Yes                           | <b>IMSI + APN + Interface</b> <ul style="list-style-type: none"> <li>PFCP packets matching IMSI, APN, and Interface are only forward listed</li> <li>RAN forward list is not applicable</li> </ul> | <b>IMSI + RAN + APN + Interface</b> <ul style="list-style-type: none"> <li>GTP-u packets matching IMSI, RAN, APN, and Interface are only forward listed</li> </ul> |
| IMSI + RAN        | ALL               | No                      | Yes                           | <b>IMSI + Interface</b> <ul style="list-style-type: none"> <li>PFCP packets matching the IMSI and Interface are only forward listed</li> <li>RAN forward list is not applicable</li> </ul>         | <b>IMSI + RAN + Interface</b> <ul style="list-style-type: none"> <li>GTP-u packets matching IMSI, RAN, and Interface are only forward listed</li> </ul>            |
| IMSI + RAN        | ALL               | Yes                     | No                            | <b>IMSI + APN</b> <ul style="list-style-type: none"> <li>PFCP packets matching the IMSI and APN are only forward listed</li> <li>RAN forward list is not applicable</li> </ul>                     | <b>IMSI + RAN + APN</b> <ul style="list-style-type: none"> <li>GTP-u packets matching the IMSI, RAN, APN are only forward listed</li> </ul>                        |
| IMSI + RAN        | ALL               | No                      | No                            | <b>IMSI</b> <ul style="list-style-type: none"> <li>PFCP packets matching the IMSI are only forward listed</li> <li>RAN forward list is not applicable</li> </ul>                                   | <b>IMSI + RAN</b> <ul style="list-style-type: none"> <li>GTP-u packets matching IMSI and RAN are only forward listed</li> </ul>                                    |

## View CUPS Communication Dashboard

The CUPS (CPN-UPN) communication dashboard captures the statistics involved when the CPN communicates with the UPN to supplement the UPN with **RAN** and **Network Slice** attributes. Refer to [CPN-UPN Communication for Support of RAN and Network Slice Attributes](#) topic for the list of supported **RAN** and **Network Slice** attributes.

To access the dashboards:

1. Go to  -> **Analytics -> Dashboards**.
2. Navigate to **Mobility Dashboards -> CUPS Communication**.
3. The **CUPS Communication** consists of Packet Statistics, GPFCP Statistics, and Enrichment Statistics.
4. Choose the required statistics tab to view the visualizations listed in the tables below.
5. Select the required Site, CPN Alias and the UPN Alias to view the CPN UPN communication statistics of a specific site.
6. When the UPN GigaSMART engine goes down, an alarm is raised and displayed in the **UPN Engine Outage** section of the CUPS Communication dashboard with **Cluster ID**, **Engine ID** of the GigaSMART engine and the **Timestamp** of the engine outage.
  - When there are zero values for all the KPIs in the **CUPS Communication** dashboard, it indicates that the UPN GigaSMART engine is down, and you can find the **Cluster ID** and the **Engine ID** of that UPN GigaSMART engine in the **UPN Engine Outage** visualization.
  - The same statistics is replicated in all the UPN GigaSMART engines that are part of the GigaSMART engine group. In the **CUPS Communication Dashboard**, GigaVUE-FM displays only the statistics of the first UPN GigaSMART engine of the engine group. When you have zero values for all the KPIs in the **CUPS Communication** dashboard, it indicates that the first UPN GigaSMART engine is down, and you can find the **Cluster ID** and the **EngineID** of that UPN GigaSMART engine in the **UPN Engine Outage** visualization.

Click the  button to download the UPN GigaSMART engine outage details in .csv format.

The following tables list the various CUPS communication statistics visualizations:

### Packet Statistics

The following table displays the visualization details of Packet Statistics.

Table 2: Packet Statistics Dashboard

| Visualizations | Details                                                           |
|----------------|-------------------------------------------------------------------|
| CPN Tx Packets | Displays the total number of packets transmitted from CPN to UPN. |
| UPN Rx Packets | Displays the total number of packets received at UPN from CPN.    |
| CPN Tx Bits    | Displays the total number of bits transmitted from CPN to UPN.    |
| UPN Rx Bits    | Displays the total number of bits received at UPN from CPN.       |

| Visualizations   | Details                                                           |
|------------------|-------------------------------------------------------------------|
| UPN Tx Packets   | Displays the total number of packets transmitted from UPN to CPN. |
| CPN Rx Packets   | Displays the total number of packets received at CPN from UPN.    |
| UPN Tx Bits      | Displays the total number of bits transmitted from UPN to CPN.    |
| CPN Rx Bits      | Displays the total number of bits received at CPN from UPN.       |
| CPN Packets Drop | Displays the total number of packets dropped at CPN.              |
| UPN Packets Drop | Displays the total number of packets dropped at UPN.              |

## Packet Statistics

The following displays the visualization details of GPFCP Statistics.

*Table 3: GPFCP Statistics Dashboard*

| Visualizations                | Details                                                                                                                                                                    |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPN GPFCP Session Lookup Fail | Counter to indicate the number of sessions not found for Enrichment update or Enrichment Pull at the CPN.                                                                  |
| UPN GPFCP Session Lookup Fail | Counter to indicate the number of sessions not found for Enrichment update or Enrichment Pull at the UPN.                                                                  |
| CPN GPFCP Ack Missing         | Displays the GPFCP acknowledgment(s) missing at CPN. If the acknowledgment is missing for an Enrichment update, regenerate Enrichment update is accounted in this counter. |
| UPN GPFCP Ack Missing         | Displays the GPFCP acknowledgment(s) missing at UPN. If the acknowledgment is missing for an Enrichment update, regenerate Enrichment update is accounted in this counter. |
| CPN GPFCP Tx HB               | Displays the GPFCP heartbeats at CPN transferred.                                                                                                                          |
| CPN GPFCP Rx HB               | Displays the GPFCP heartbeats at CPN received.                                                                                                                             |
| UPN GPFCP Rx HB               | Displays the GPFCP heartbeats at UPN received.                                                                                                                             |
| UPN GPFCP Tx HB               | Displays the GPFCP heartbeats at UPN transferred.                                                                                                                          |

## Enrichment Statistics

The following table displays the visualization details of Enrichment Statistics.

*Table 4: Enrichment Statistics Dashboard*

| Visualizations                    | Details                                                                        |
|-----------------------------------|--------------------------------------------------------------------------------|
| CPN Tx Enrichment Update          | Displays the number of Enrichment update messages transmitted from CPN to UPN. |
| UPN Rx Enrichment Update          | Displays the number of Enrichment update messages received at UPN from CPN.    |
| UPN Tx Enrichment Response Accept | Displays the number of acknowledgment messages transmitted from the            |

| Visualizations                       | Details                                                                                                                                                                                                                                                                                             |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                      | UPN to the CPN for an Enrichment update stating that the update is accepted.                                                                                                                                                                                                                        |
| CPN RX Enrichment Response Accept    | Displays the number of acknowledgment messages received at CPN from UPN for a n Enrichment update stating the update is accepted.                                                                                                                                                                   |
| UPN Tx Enrichment Response Reject    | Displays the number of acknowledgment messages transmitted from the UPN to the CPN for an Enrichment update stating that the update is rejected.                                                                                                                                                    |
| CPN Rx Enrichment Response Reject    | Displays the number of acknowledgment messages received at CPN from the UPN for an Enrichment update stating that the update is rejected.                                                                                                                                                           |
| UPN Tx Enrichment Pull Request       | Displays the number of Enrichment Pull Request messages transmitted from UPN (UPN tries to get RAN and Network Slice attributes from the CPN).                                                                                                                                                      |
| CPN Rx Enrichment Pull Request       | Displays the number of Enrichment Pull Request messages received at CPN (CPN receives the pull request from the UPN for the RAN and Network Slice attributes).                                                                                                                                      |
| UPN Tx Enrichment Pull Request Retry | Displays the number of Enrichment Pull Request Retry messages transmitted from UPN.<br><br><b>Note:</b> When CPN does not respond to the Enrichment Pull Request from UPN, it sends the UPN Tx Enrichment Pull Request Retry message. The maximum number of retries that can be attempted is three. |
| CPN Enrichment Retry                 | Displays the number of Enrichment Retry messages transmitted from CPN (CPN retries to enrich the UPN for a REJECTED acknowledgment from UPN).                                                                                                                                                       |

### Rollback from CPN-UPN Communication Solution to Standalone UPN

This section provides the steps to rollback from CPN-UPN Communication Solution to Standalone UPN and also clean up the configurations performed for the CPN-UPN Communication solution. If the CPN-UPN Communication fails due to some issues, you can roll back to the previous Standalone UPN Solution.

Follow the steps given below to roll back to Standalone UPN:

| Step No | Task                                                             | Refer the following topics   |
|---------|------------------------------------------------------------------|------------------------------|
| 1.      | Remove CPN specific second level maps                            | <a href="#">map</a>          |
| 2.      | Remove <b>vports</b> configured for CPN                          | <a href="#">vport</a>        |
| 3.      | Delete the first level maps configured for <b>gpfcp</b> messages | <a href="#">map</a>          |
| 4.      | Delete other CPN specific first level maps                       | <a href="#">map</a>          |
| 5.      | Delete <b>gsops</b> attached to the CPN engine                   | <a href="#">gsop</a>         |
| 6.      | Delete <b>IP interfaces</b> for CPN UPN communication            | <a href="#">ip interface</a> |
| 7.      | Delete the CPN <b>gsgroup</b>                                    | <a href="#">gsgroups</a>     |
| 8.      | Remove <b>gpfcp</b> profile from UPN <b>gsparams</b>             | <a href="#">gsparams</a>     |

| Step No | Task                                                                                   | Refer the following topics    |
|---------|----------------------------------------------------------------------------------------|-------------------------------|
| 9       | Remove the <b>exporter</b> configurations for both the CPN and UPN                     | <a href="#">apps exporter</a> |
| 10      | Delete all the configured <b>gpfcf</b> profiles                                        | <a href="#">gpfcf profile</a> |
| 11      | Remove <b>RAN</b> and <b>Network Slicing</b> rules from UPN specific second level maps | <a href="#">map rule</a>      |

### Quick Rollback from CPN-UPN Communication Solution to Standalone UPN

This section provides the steps to rollback from CPN-UPN Communication Solution to Standalone UPN without deleting the configurations created for CPN-UPN Communication Solution. The quick rollback will be handy while debugging issues in the CPN-UPN Communication Solution.

Follow the steps given below to perform quick roll back to Standalone UPN Solution:

1. Remove **gpfcf** profile from UPN **gsparams**. Refer to [gsparams](#) for more detailed instructions.
2. Remove **gpfcf** profile from CPN **gsparams**. Refer to [gsparams](#) for more detailed instructions.

### Monitoring of Subscriber Intelligence Solutions

You can monitor the following solution in GigaVUE-FM after configuring the solution through Ansible:

- [Monitoring CUPS Solution](#)

#### Monitoring CUPS Solution

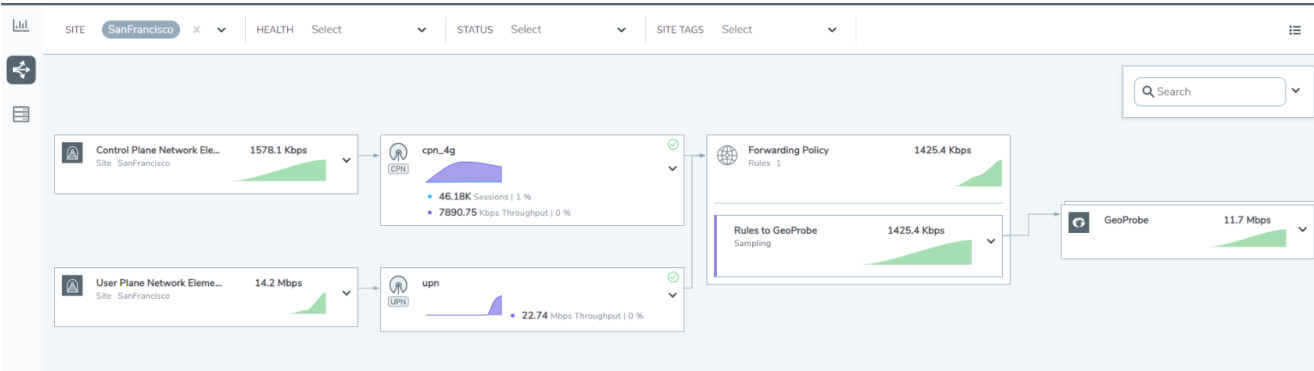
You can monitor the CUPS solution in GigaVUE-FM after configuring the solution through Ansible. You can monitor the following information from GigaVUE-FM:

- Interface
- CPN-UPN
- Forwarding Policies
- Tool

To view the CUPS solution, follow these steps:

1. Go to **Traffic**  .
2. Go to **Physical > Orchestrate > Mobility**.
3. Select a Site from the **SITE** drop-down list. If required, you can select multiple sites.

The screen appears as shown in the figure:



GigaVUE-FM also helps you to view the statistics and health information of the following:

| Components          | Statistics and Health Information for...                             |
|---------------------|----------------------------------------------------------------------|
| CPN-UPN function    | First level fabric maps                                              |
| CPN-UPN node        | GigaSMART Group, SFFP Profile, Exporter, Listener, and IP interface. |
| Forwarding Policies | GSOPS and Second level Map.                                          |

To view the statistics and health information, follow these steps:

1. Go to **Physical > Orchestrate > CUPS**.
2. Select a **Site** from the SITE drop-down list.
3. Select a component from the GUI.
4. Click **Troubleshoot** to view the statistics and health information.

Health Status of Solution

Health Status of a Solution depends on the health status of the CPN and UPN configured in the solution.

The health status of a solution is indicated by the following colors:

| Color | Health Status of Solution CPN/UPN Node State                                                          |
|-------|-------------------------------------------------------------------------------------------------------|
| Green | Healthy -All the CPNs and UPNs health node status are green                                           |
| Amber | Partially Healthy- None of the CPNs/UPNs nodes is red or at least a node is not functioning properly. |
| Red   | Unhealthy- At least one None of the CPNs/UPNs node is not functioning properly.                       |

CPN Health State

A single CPN's health is based on the health of following components configured in the CPN:

- Source Ports for CPN
- First Level Maps
- GigaSMART (vport, gsgroup and GSOP)
- Second Level Maps
- Destination Tools Ports
- CPN IP Interface

**NOTE:** Only active CPNs are considered in health computation.

## UPN Health State

A single UPN's health is based on the health of following components configured in the UPN:

- Source Ports for UPN
- First Level Maps
- GigaSMART (vport, Gsgroup and gsop)
- Second Level Maps
- DestinationTools Ports
- UPN IpInterface

**NOTE:** Only Active UPNs are considered in health computation.

The following table explains the health status of a CPN/UPN in GigaVUE-FM based on the health status of the components configured in the CPN/UPN:

| Color | UPN Health State                                                                                                    |
|-------|---------------------------------------------------------------------------------------------------------------------|
| Green | Healthy - All the above components of the CPN/UPN are successfully configured.                                      |
| Amber | Partially Healthy-None of the components or any of the CPN/UPN component is not successfully configured.            |
| Red   | Unhealthy- At least one or any of the configuration status of the CPN/UPN component is not successfully configured. |

### Monitor Session and Tunnel Utilization

This section describes how to monitor Session and Tunnel utilization of GigaSMART engines configured in a Subscriber Intelligence Solution.

### Configure SNMP Traps for Subscriber Intelligence Solution

Real-time alerts for key resource and performance indicators within GTP engines can be accessed, such as:

- **Engine Approaching Tunnel/Session Limits** : Alerts are generated when tunnel or session usage nears capacity
- **GTP Persistence Restore Failure**: Notifications are sent if the persistence file is stale or corrupted.
- **Low Mempool Packet Buffers** : Alerts indicate when packet buffer availability is running low.
- **High CPU Utilization**: Notifications are triggered as CPU usage approaches a user-defined threshold.

These alerts enhance visibility into system health, allowing for more efficient troubleshooting and operational oversight.

These alerts are generated once the said resource parameter is enabled in the GigaSMART Group. To enable these configuration follow the below steps:

- From the left navigation pane, go to **Inventory > Physical > Nodes**.
- Select the node, and then go to **GigaSMART > GigaSMART Groups> GigaSMART Parameters**.
- The GigaSMART Group parameters that need to be enabled are as follows:
  - **Enable Resource Packet Buffer** - This allows configuration of Packet Buffer Usage Threshold values. A clear alert is triggered when the packet buffer usage falls 20% below the high threshold value.
  - **Enable Tunnel Usage Threshold-** .This enables the configuration of tunnel usage thresholds. After enabling, configure the threshold values in the **Maximum Tunnel Usage Threshold** field within the range of 50-90%. The default value is 90%. If tunnel usage exceeds this configured value, an SNMP trap will be generated. A clear trap will be sent when the tunnel utilization drops to 10% below the high threshold value.
  - **Enable Session Usage Threshold-** This allows configuration of session usage thresholds. After enabling, configure the threshold values in the **Maximum Session Usage Threshold** field within the range of 50-90%. The default value is 90%. If session usage exceeds this configured value, an SNMP trap will be generated. A clear trap will be sent when session utilization drops to 10% below the high threshold value.
  - **GTP Persistence-** This allows configuration of GTP Persistence timer values. Refer to [GTP Stateful Session Recovery](#) to know more.
  - **Enable Resource CPU Utilization** -This allows the configuration of CPU utilization threshold values. A clear alert will be triggered when the CPU utilization drops below two-thirds of the high percentage value.

Additionally, these threshold values can also be configured through the GigaVUE-OS CLI refer to [snmp-server](#) and [gsparams](#) in GigaVUE-OS CLI Reference Guide

Once these values are configured in the GigaSMART Group, it is possible to enable the required event for SNMP notifications either on the device or on the GigaVUE-FM instance managing the device. For instructions about how to enable SNMP notification on a device, refer to [Enable or Disable Events for SNMP Notifications](#) in GigaVUE-Administration Guide.

To view the SNMP trap ,its corresponding Object Identifier and Events refer to [Mapping of SNMP Traps with GigaVUE-FM Events and Alarms](#) in the GigaVUE-Administration Guide.

The threshold values for sessions can also be visualized under the Analytics tab Refer to [Analytics](#).

| SOURCE      | TIME                | EVENT TYPE                                                 | SEVERITY | AFFECTED ENTITY TYPE | AFFECTED ENTITY | CLUSTER ID  | ALIAS       | DEVICE ID   | HOST NAME | SCOPE   | DESCRIPTION                                                                                                                                    |
|-------------|---------------------|------------------------------------------------------------|----------|----------------------|-----------------|-------------|-------------|-------------|-----------|---------|------------------------------------------------------------------------------------------------------------------------------------------------|
| FM          | 2025-01-20 20:54:21 | Alarm Create Event                                         | Critical | Gigasmart group      | gsgp1           | 10.114.74.3 | gsgp1       |             |           | Alarm   | For the port [10/34/1] mobility Session utilization exceeded the threshold of [90%].                                                           |
| FM          | 2025-01-20 20:54:21 | Alarm Create Event                                         | Critical | Map                  | gpb_hu.v1.e     | 10.114.74.3 | gpb_hu.v1.e |             |           | Alarm   | VPORT component(s) v1 are unhealthy as underlying GigaSMART engine parts might be down or experiencing packet drop/errors or low packet con... |
| FM          | 2025-01-20 20:54:21 | Alarm Create Event                                         | Critical | Map                  | gpb_fm          | 10.114.74.3 | gpb_fm      |             |           | Alarm   | VPORT component(s) v1 are unhealthy as underlying GigaSMART engine parts might be down or experiencing packet drop/errors or low packet con... |
| FM          | 2025-01-20 20:54:21 | Alarm Create Event                                         | Critical | Map                  | gpb_hu.v1.u     | 10.114.74.3 | gpb_hu.v1.u |             |           | Alarm   | VPORT component(s) v1 are unhealthy as underlying GigaSMART engine parts might be down or experiencing packet drop/errors or low packet con... |
| FM          | 2025-01-20 20:54:21 | Alarm Create Event                                         | Critical | Virtual Port         | v1              | 10.114.74.3 | v1          |             |           | Alarm   | Component(s) gsgp1 parts are experiencing packet drop/errors or admin disabled.                                                                |
| FM          | 2025-01-20 20:54:21 | Alarm Create Event                                         | Critical | Port                 | [34/1]          | 10.114.74.3 |             | dev1        |           | Alarm   | Session utilization exceeds the threshold limit [90%]                                                                                          |
| 10.114.74.3 | 2025-01-20 20:54:21 | GigaSMART Mobility Resource Session Overload Status Change | Critical | Gigasmart group      |                 | 10.114.74.3 |             | 10.114.74.3 | dev1      | phyNode | For the port [10/34/1] mobility Session utilization exceeded the threshold of [90%]                                                            |
| FM          | 2025-01-20 21:20:45 | Alarm Delete Event                                         | Critical | Gigasmart group      | gsgp1           | 10.114.74.3 | gsgp1       |             |           | Alarm   | For the port [10/34/1] mobility Session utilization exceeded the threshold of [90%].                                                           |
| FM          | 2025-01-20 21:20:45 | Alarm Delete Event                                         | Critical | Map                  | gpb_hu.v1.e     | 10.114.74.3 | gpb_hu.v1.e |             |           | Alarm   | VPORT component(s) v1 are unhealthy as underlying GigaSMART engine parts might be down or experiencing packet drop/errors or low packet con... |
| FM          | 2025-01-20 21:20:45 | Alarm Delete Event                                         | Critical | Map                  | gpb_fm          | 10.114.74.3 | gpb_fm      |             |           | Alarm   | VPORT component(s) v1 are unhealthy as underlying GigaSMART engine parts might be down or experiencing packet drop/errors or low packet con... |
| FM          | 2025-01-20 21:20:45 | Alarm Delete Event                                         | Critical | Map                  | gpb_hu.v1.u     | 10.114.74.3 | gpb_hu.v1.u |             |           | Alarm   | VPORT component(s) v1 are unhealthy as underlying GigaSMART engine parts might be down or experiencing packet drop/errors or low packet con... |
| FM          | 2025-01-20 21:20:45 | Alarm Delete Event                                         | Critical | Virtual Port         | v1              | 10.114.74.3 | v1          |             |           | Alarm   | Component(s) gsgp1 parts are experiencing packet drop/errors or admin disabled.                                                                |
| FM          | 2025-01-20 21:20:44 | Alarm Delete Event                                         | Critical | Port                 | [34/1]          | 10.114.74.3 |             | dev1        |           | Alarm   | Session utilization exceeds the threshold limit [90%]                                                                                          |
| 10.114.74.3 | 2025-01-20 21:20:44 | GigaSMART Mobility Resource Session Overload Status Change | Critical | Gigasmart group      |                 | 10.114.74.3 |             | 10.114.74.3 | dev1      | phyNode | For the port [10/34/1] mobility Session utilization is normal.                                                                                 |

## Upgrade Standalone UPN to CPN-UPN Communication Solution

To upgrade your existing Standalone UPN solution to CPN-UPN Communication solution, follow the steps given below:

| Step No | Task                                                                  | Refer the following topics    |
|---------|-----------------------------------------------------------------------|-------------------------------|
| 1.      | Configure CPN <b>gsgroup</b>                                          | <a href="#">gsgroups</a>      |
| 2.      | Configure <b>gpfc</b> profiles for both CPN and UPN                   | <a href="#">gpfc profile</a>  |
| 3.      | Configure <b>IP-Interface</b> for CPN-UPN communication               | <a href="#">ip interface</a>  |
| 4.      | Add <b>exporters</b> to both CPN and UPN                              | <a href="#">apps exporter</a> |
| 5.      | Add the configured <b>gpfc</b> profiles to <b>gsparams</b>            | <a href="#">gsparams</a>      |
| 6.      | Configure <b>gpfc delay-interval</b> for CPN                          | <a href="#">gpfc profile</a>  |
| 7.      | Add <b>gsop</b> for the CPN                                           | <a href="#">gsop</a>          |
| 8.      | Add <b>vport</b> for the CPN                                          | <a href="#">vport</a>         |
| 9.      | Configure first level maps for the CPN                                | <a href="#">map</a>           |
| 10.     | Add first level maps for sending gpfc messages to CPN and UPN engines | <a href="#">map</a>           |
| 11.     | Configure second level maps for CPN                                   | <a href="#">map</a>           |
| 12.     | Configure or edit second level maps for UPN                           | <a href="#">map</a>           |

## Display Flow Ops Reports

GigaSMART provides support for Flow Ops reporting. The Flow Ops reports display session table statistics for the various features. Refer to [GigaSMART Group Statistics Definitions](#) for descriptions of these statistics.

To display the Flow Ops report perform the following steps:

1. From the device view, select **GigaSMART > GigaSMART Groups > Report**.
2. Under **Report Info**, from the **Type** drop down list, select any one of the following report types to display the respective reports:
  - **Flow Filtering**- Flow Filtering reports.
  - **Flow Sampling** - Flow Sampling reports.
  - **Flow SIP** - Flow SIP reports.
  - **SSL Decryption** - SSL Decryption reports.
  - **Port Throttling** Port Session and Port Throttle reports.

**NOTE:** For information about the fields that get displayed for each of the report type, refer to "Flow Ops Report - Field Reference"

3. Select a GigaSMART Group - for example: **grp1**.
4. Click **Generate**.

The corresponding Flow Ops report appears with the time stamp of when the report was generated. The field labels and the values selected (or entered) for generating the report appear as sticky info notes in the header pane. The following buttons are available in the header pane:

- **Generate New:** Use to generate a new report and to toggle between the report generated and the Reports page.
- **Export:** Use to export the report.
- **Upload:** Use to upload the report to the archive server.

**NOTE:** The IP based Flow Sampling reports cannot be exported or uploaded. To upload IP based flow sample report use GigaVUE-OS CLI commands:  
`show gsgroup flow-ops-report alias <> type flow-sampling any upload`  
`show gsgroup flow-ops-report alias <> type flow-sampling device-ip-mask <netmask> upload`  
`show gsgroup flow-ops-report alias <> type flow-sampling device-ip6-mask <upload>`  
Refer to showcommand in GigaVUE-OS CLI Reference Guide, and [Definitions of GigaSMART Statistics](#)

Report Generated at 11:30:00 28/08/2023

Session Summary   GTP Session   GTP Interface   GTP Correlation   **GTP PFCP**

▼ GTP PFCP Statistics

| Message Type                            | Packet Count |
|-----------------------------------------|--------------|
| Heart Beat Request                      | 24           |
| Heart Beat Response                     | 24           |
| PFD Management Request                  | 0            |
| PFD Management Response                 | 0            |
| Association Setup Request               | 3            |
| Association Setup Response              | 3            |
| Association Update Request              | 0            |
| Association Update Response             | 0            |
| Association Release Request             | 1            |
| Association Release Response            | 1            |
| Version Not Supported Response          | 0            |
| Node Report Request                     | 0            |
| Node Report Response                    | 0            |
| Session Set Deletion Request            | 0            |
| Session Set Deletion Response           | 0            |
| Reserve Message Type of range 16 to 49  | 0            |
| Reserve Message Type of range 58 to 255 | 0            |
| Bundled Message                         | 0            |

**Flow Ops Report - Field Reference**

| Report Type    | Fields                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Flow Filtering | <ul style="list-style-type: none"> <li>• <b>Pattern</b></li> <li>• <b>Any</b></li> </ul> | <ul style="list-style-type: none"> <li>• <b>Pattern:</b> Pattern for which the Flow Filtering report must be generated. The <b>Pattern</b> drop-down lists the following options. <ul style="list-style-type: none"> <li>• GTP IMSI</li> <li>• GTP IMEI</li> <li>• GTP MSISDN</li> </ul> </li> </ul> <p>Enter the required value for the selected option. The report is generated accordingly.</p> <ul style="list-style-type: none"> <li>• <b>Any-</b>Select <b>Any</b> for any of the patterns to be selected.</li> </ul> <p><b>Note:</b> The patterns and sub-pattern options are specific to device versions and may change accordingly.</p> | <p>The Flow Filtering report appears as a single page with links to the various sections of the report. Click on the links to navigate to the following sections:</p> <ul style="list-style-type: none"> <li>• Session Summary</li> <li>• GTP Session Statistics</li> <li>• GTP Interface Statistics</li> <li>• GTP Correlation Statistics</li> <li>• GTP PFCP Statistics</li> </ul> <p>The report generation time is displayed on top of the report.</p> <p>Refer to the following sections for details:</p> <ul style="list-style-type: none"> <li>• <a href="#">Export Flow Filtering Reports</a></li> <li>• <a href="#">Generate Delta Reports</a></li> </ul> <p><b>Note:</b> In the Hand Over scenario, the flow-ops report does not reflect the entire gtp-u packet count, since the older tunnels are marked for free before the sync mechanism starts between the leader and non-leader engines. The packets that are sent to the older tunnels are not taken into account in the flow-ops report.</p> <p><b>Note:</b> When RAN attributes are not</p> |

| Report Type    | Fields                                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Notes                                                                                                                                                                                                             |
|----------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                           | <ul style="list-style-type: none"> <li>• <b>Duration:</b> Time at which the Flow Filtering report needs to be generated. The following options are available: <ul style="list-style-type: none"> <li>• <b>Now:</b> Report with current statistical data is generated. This is the default option.</li> <li>• <b>Delta:</b> Report with statistical data for a specified time interval starting from the current time is generated. Select the required duration: <ul style="list-style-type: none"> <li>• 5 minutes</li> <li>• 15 minutes</li> <li>• 30 minutes</li> <li>• 1 hour</li> <li>• 4 hours</li> <li>• 12 hours</li> <li>• 1 day</li> <li>• 2 days</li> <li>• 7 days</li> </ul> </li> </ul> </li> </ul> | exchanged from CPN to UPN, the RAN metrics, such as ECI, TAC, and NSI_SST are displayed as zero in the flow-ops report. No values are displayed for other RAN metrics such as TMCC, TMNC, EMCC, EMNC, and NSI_SD. |
| Flow Sampling  | <ul style="list-style-type: none"> <li>• Device IP Address/Mask</li> <li>• Any</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Device IP Address/Mask</b> - Device IP address/Mask.</li> <li>• <b>Any</b>- Select <b>Any</b> for any available device IP address.</li> </ul> <p><b>Note:</b> Graphs will not be generated for Device IP Address /Mask.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          | Use the scroll bars and the pagination option at the bottom of the page to navigate to the various pages.                                                                                                         |
| Flow SIP       | <ul style="list-style-type: none"> <li>• Caller ID Pattern</li> <li>• Any</li> </ul>      | <ul style="list-style-type: none"> <li>• <b>Caller ID Pattern</b> - Caller ID pattern.</li> <li>• <b>Any</b>- Select <b>Any</b> for any available device IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                   |
| SSL Decryption | <ul style="list-style-type: none"> <li>• Device IP Address/Mask</li> <li>• Any</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Device IP Address/Mask</b> - Device IP address/Mask.</li> <li>• <b>Any</b>- Select <b>Any</b> for any available device IP address.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                   |

## Export Flow SIP Session Reports

Support for exporting flow-ops session report is available for Flow SIP. To export Flow SIP session reports:

1. From the device view, select **GigaSMART > GigaSMART Groups > Report**.
2. Generate a Flow SIP report.
3. Click **Export** to download the Flow SIP report you just generated. A text file of the Flow SIP report is saved to your local directory.

**NOTE:** The session table displays the first 1000 sessions only.

flowSipReport (2) - Notepad

| PROTO | TRANSPORT | METHOD | CALLER:IP                                             | CALLEE:IP                                                                         | PDU | CALL-ID                     | wL | FS | LB port |
|-------|-----------|--------|-------------------------------------------------------|-----------------------------------------------------------------------------------|-----|-----------------------------|----|----|---------|
| SIP   | UDP       | PRACK  | 16127500192<br>2600:1014:1117:f3f:c284:4bd2:b621:680e | 6513012997<br>2001:4888:2:fe40:a0:104:0:265                                       | 5   | 9FsyjtyxrAlgwnv8N_8y0A..@26 | N  | A  | -       |
| SIP   | UDP       | PRACK  | 13175901000<br>2001:4888:2:fe40:a0:104:0:271          | 16127500192:npdi<br>2600:1014:110b:2b28:99f0:ee92:2124:bf12                       | 2   | LU-1507640551275087-1220667 | N  | A  | -       |
| SIP   | UDP       | PRACK  | 15173459109<br>2001:4888:2:fe40:a0:104:0:271          | 16127500192:npdi<br>2600:1014:110b:2b28:99f0:ee92:2124:bf12                       | 57  | ak5q9ic-f81dee*LU-150783467 | N  | A  | -       |
| SIP   | UDP       | INVITE | 16513012997<br>2001:4888:202:3f40:a0:104:0:291        | 16127500192<br>2001:4888:202:70ff:a0:113::                                        | 2   | p65546t1507652897m818029c34 | N  | A  | -       |
| RTP   | UDP       |        | 2600:1008:1114:31a9:71e0:1a36:f936:92ca               | unknown:0                                                                         | 0   |                             |    |    |         |
| RTCP  | UDP       |        | 2600:1008:1114:31a9:71e0:1a36:f936:92ca               | unknown:1                                                                         | 0   |                             |    |    |         |
| SIP   | UDP       | PRACK  | 14074884255<br>2001:4888:2:fe40:a0:104:0:26e          | 16127500192:npdi<br>2600:1014:1101:2d8e:e38d:e74:f2e:1f18                         | 2   | ak5q9ic-8e0ab9*LU-150756420 | N  | A  | -       |
| SIP   | UDP       | PRACK  | 16123669520<br>2001:4888:2:fe40:a0:104:0:26e          | 16127500192:npdi;phone-context=nodomain.<br>2600:1014:1101:2d8e:e38d:e74:f2e:1f18 | 5   | ak5q9ic-c59071*LU-150747960 | N  | A  | -       |
| SIP   | UDP       | PRACK  | 14254661456<br>2001:4888:2:fe40:a0:104:0:271          | 16127500192:npdi<br>2600:1014:110b:2b28:99f0:ee92:2124:bf12                       | 23  | ak5q9ic-125f5e*LU-150781540 | N  | A  | -       |
| SIP   | UDP       | PRACK  | 16513012997<br>2001:4888:2:fe40:a0:104:0:271          | 16127500192:npdi<br>2600:1014:110b:2b28:99f0:ee92:2124:bf12                       | 2   | ak5q9ic-6628ad*LU-150758881 | N  | A  | -       |
| SIP   | UDP       | INVITE | 16123669520<br>172.18.135.199                         | 11916127500192;phone-context=nodomain.co<br>172.27.228.244                        | 58  | 122718103327211137874590681 | N  | A  | -       |
| RTP   | UDP       |        | Unknown:0                                             | 172.27.212.212:51368                                                              | 0   |                             |    |    |         |
| RTCP  | UDP       |        | Unknown:1                                             | 172.27.212.212:51369                                                              | 0   |                             |    |    |         |
| RTP   | UDP       |        | Unknown:0                                             | 2001:4888:39:ff01:308:10d:0:10:54058                                              | 0   |                             |    |    |         |
| RTCP  | UDP       |        | Unknown:1                                             | 2001:4888:39:ff01:308:10d:0:10:54059                                              | 0   |                             |    |    |         |
| RTP   | UDP       |        | 2001:4888:39:ff00:308:106:0:a:44878                   | unknown:0                                                                         | 0   |                             |    |    |         |
| RTCP  | UDP       |        | 2001:4888:39:ff00:308:106:0:a:44879                   | unknown:1                                                                         | 0   |                             |    |    |         |
| RTP   | UDP       |        | 172.17.13.51:37682                                    | unknown:0                                                                         | 0   |                             |    |    |         |
| RTCP  | UDP       |        | 172.17.13.51:37683                                    | unknown:1                                                                         | 0   |                             |    |    |         |
| SIP   | UDP       | PRACK  | 16123669520<br>2001:4888:2:fe40:a0:104:0:26e          | 16127500192:npdi;phone-context=nodomain.<br>2600:1014:1101:2d8e:e38d:e74:f2e:1f18 | 9   | ak5q9ic-43f96d*LU-150757237 | N  | A  | -       |

## Export Flow Filtering Reports

Support for exporting the flow filtering report is available.

To export Flow Filtering reports:

1. From the device view, select **GigaSMART > GigaSMART Groups > Report**.
2. Generate a Flow Filtering Report.
3. Click **Export** to download the Flow Filtering report you just generated. An excel sheet of the Flow Filtering report is saved to your local directory.

|    | A                  | B                   | C                      | D                       | E                         | F                          | G                          | H                           | I                           | J                            | K                          | L                   | M                    | N                            | O                             | P                                      | Q                                       | R               | S | T | U |
|----|--------------------|---------------------|------------------------|-------------------------|---------------------------|----------------------------|----------------------------|-----------------------------|-----------------------------|------------------------------|----------------------------|---------------------|----------------------|------------------------------|-------------------------------|----------------------------------------|-----------------------------------------|-----------------|---|---|---|
|    | Heart Beat Request | Heart Beat Response | PFD Management Request | PFD Management Response | Association Setup Request | Association Setup Response | Association Update Request | Association Update Response | Association Release Request | Association Release Response | Version Supported Response | Node Report Request | Node Report Response | Session Set Deletion Request | Session Set Deletion Response | Reserve Message Type of range 16 to 49 | Reserve Message Type of range 58 to 255 | Bundled Message |   |   |   |
| 1  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 2  | 24                 | 24                  | 0                      | 0                       | 3                         | 3                          | 0                          | 0                           | 0                           | 1                            | 1                          | 0                   | 0                    | 0                            | 0                             | 0                                      | 0                                       | 0               |   |   |   |
| 3  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 4  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 5  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 6  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 7  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 8  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 9  |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 10 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 11 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 12 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 13 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 14 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 15 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 16 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 17 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 18 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 19 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |
| 20 |                    |                     |                        |                         |                           |                            |                            |                             |                             |                              |                            |                     |                      |                              |                               |                                        |                                         |                 |   |   |   |

**NOTE:** The excel sheet contains separate tabs for each of the sections in the report.

Generate Delta Reports

GigaVUE-FM provides support for generating delta reports that display statistical data for a specific time interval from the current time. Use delta reports to troubleshoot the flow filtering behavior across two different timestamps.

To generate a delta report:

1. From the device view, select **GigaSMART > GigaSMART Groups > Report**.
2. Select or enter the following details:
  - **Pattern:** Select the required pattern or choose any.
  - **Duration:** Select the required duration.

Refer to the [Flow Ops Report - Field Reference](#) section for details.

The screenshot displays the 'GigaSMART Groups' report configuration page. The left sidebar contains a navigation menu with options like 'Back to Nodes', 'Overview', 'Health', 'Save Configuration', and a 'SYSTEM' section with various sub-items including 'GigaSMART Groups'. The main content area is titled 'Report Info' and includes the following fields:

- Type \***: A dropdown menu currently set to 'Flow Filtering'.
- GigaSMART Groups \***: A dropdown menu currently set to 'gsop1'.
- Pattern**: A dropdown menu currently set to 'Select pattern'.
- Type**: Radio buttons for 'Now' and 'Delta', with 'Delta' selected.
- Duration \***: A dropdown menu currently set to '15 minutes', with a list of other options (10 minutes, 30 minutes, 1 hour, 4 hours, 12 hours, 1 day, 2 days) visible below it.

At the top right of the main area, there are 'Generate' and 'Upload' buttons. The bottom status bar shows 'FM Instance: GigaVUE-FM - 6.10.00', 'Device version: 6.9.00\_Beta', 'Attempted Sync Time: Feb 12, 2025 15:16:41', and 'Successful Sync Time: Feb 12, 2025 15:16:41'.

3. Click **Generate**. The delta report for the selected duration is displayed. The following details are displayed as part of the report:
  - Duration of the delta report in the page header
  - Detailed timestamps as part of the report header
  - Within the report, the following details are displayed:
    - **Old:** Earliest record available based on the duration selected. For example, if the duration is selected as 12 hours, the oldest data available for the past 12 hours from the current time is displayed.
    - **New:** Latest record available for the selected duration. The latest record displayed is based on the last stats collection in GigaVUE-FM, GigaVUE HC Series and sometimes may not be the latest value on the device due to the stats collection interval.
    - **Delta:** Differential data calculated for the selected duration is displayed.

**NOTE:** Negative values in the delta columns indicate that a device reset or maintenance has occurred between the selected duration. Refer to the Old and New columns for the statistical rate change.

- Use the Export button to export the Flow Filtering report in .XLSX format. The format of the filename is as follows:

***Delta\_Report\_<GigaSMART Group name>\_<start time in YYYYMMDDHHmmss>\_<end time in YYYYMMDDHHmmss>***

The following are the sample Flow Filtering delta reports:

| Delta_Report_grp1_4g_20220417212612_20220418212612 |               |     |       |               |     |       |             |     |       |             |     |       |            |     |       |                      |     |       |     |     |       |     |     |       |     |     |       |
|----------------------------------------------------|---------------|-----|-------|---------------|-----|-------|-------------|-----|-------|-------------|-----|-------|------------|-----|-------|----------------------|-----|-------|-----|-----|-------|-----|-----|-------|-----|-----|-------|
| GTP Interface                                      |               |     |       |               |     |       |             |     |       |             |     |       |            |     |       |                      |     |       |     |     |       |     |     |       |     |     |       |
| 1                                                  | GTP Interface |     |       | Total Bytes ( |     |       | Sample/Forw |     |       | Sample/Forw |     |       | Sample Out |     |       | Sample Out (Dropped) |     |       |     |     |       |     |     |       |     |     |       |
| 2                                                  | Old           | New | Delta | Old           | New | Delta | Old         | New | Delta | Old         | New | Delta | Old        | New | Delta | Old                  | New | Delta | Old | New | Delta | Old | New | Delta | Old | New | Delta |
| 3                                                  | Call (C)      | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 4                                                  | Call (U)      | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 5                                                  | Gn (C)        | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 6                                                  | Gn (U)        | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 7                                                  | S11           | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 8                                                  | S11u          | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 9                                                  | S1u           | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 10                                                 | S2b (C)       | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 11                                                 | S2b (U)       | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 12                                                 | SS58 (C)      | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 13                                                 | SS58 (U)      | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 14                                                 | Total (C)     | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 15                                                 | Total (U)     | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |
| 16                                                 | Xaul Drop     | 0   | 0     | 0             | 0   | 0     | 0           | 0   | 0     | 0           | 0   | 0     | 0          | 0   | 0     | 0                    | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     | 0   | 0   | 0     |

|    | A                  | B   | C     | D                   | E   | F     | G                      | H   | I     | J                       | K   | L     | M                          | N   | O     | P                           | Q   | R     |
|----|--------------------|-----|-------|---------------------|-----|-------|------------------------|-----|-------|-------------------------|-----|-------|----------------------------|-----|-------|-----------------------------|-----|-------|
| 1  | Heart Beat Request |     |       | Heart Beat Response |     |       | PFD Management Request |     |       | PFD Management Response |     |       | Associati on Setup Request |     |       | Associati on Setup Response |     |       |
| 2  | Old                | New | Delta | Old                 | New | Delta | Old                    | New | Delta | Old                     | New | Delta | Old                        | New | Delta | Old                         | New | Delta |
| 3  | 0                  | 20  | 20    | 0                   | 20  | 20    | 0                      | 0   | 0     | 0                       | 0   | 0     | 0                          | 2   | 2     | 0                           | 2   |       |
| 4  |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 5  |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 6  |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 7  |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 8  |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 9  |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 10 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 11 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 12 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 13 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 14 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 15 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |
| 16 |                    |     |       |                     |     |       |                        |     |       |                         |     |       |                            |     |       |                             |     |       |

⏪

⏩

⋮

GTP Interface Statistics

GTP Correlation Statistics

GTP-U Statistics

GTP PCFP Statistics

+

⋮

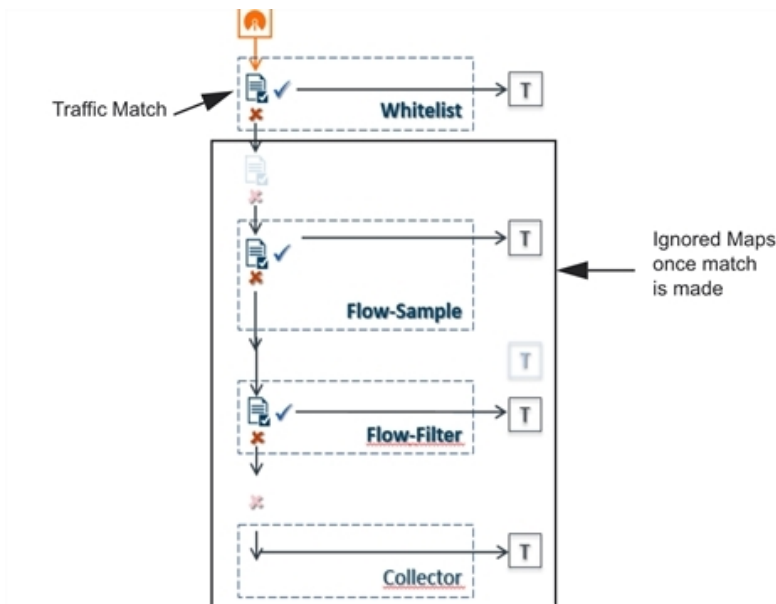
⏪

## GTP Overlap Flow Sampling Maps

Starting in software version 4.8, GTP overlap flow sampling maps combines GTP forward listing and GTP flow sampling maps into a GTP overlap flow sampling map group, which allows for selected traffic to be sent to multiple destinations simultaneously.

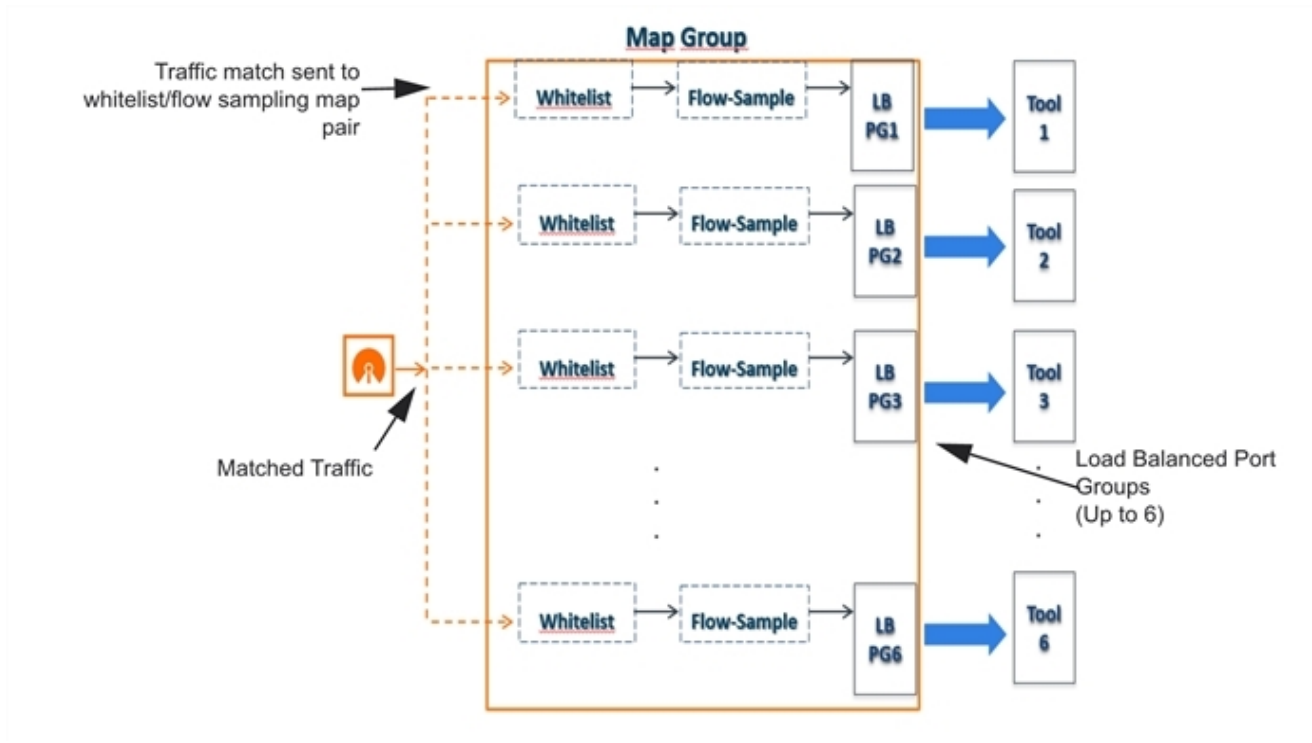
In this scenario, once traffic matches a map, it will be sent to the destination for that map. However, the matched traffic will also be evaluated by subsequent maps and, if a match occurs, it will be sent to each of the destinations pointed to by the subsequent maps.

[Figure 26GTP Overlap Flow Sampling Map Groups](#) illustrates regular non-overlap mapping where, once a traffic match is achieved in one map, all other maps are ignored.



**Figure 25** Non-Overlap GTP Mapping Mode

This contrasts with GTP overlap flow sampling maps. In [Figure 25Non-Overlap GTP Mapping Mode](#) matched traffic is sent to up to six GTP forward listing and flow sampling map pairs that in turn send accepted traffic to up to six load balanced port groups.



**Figure 26** GTP Overlap Flow Sampling Map Groups

#### Configure GTP Overlap Mapping

The configuration of GTP forward listing and GTP flow sampling maps that are part of the GTP overlap flow sampling map group follow the same configuration considerations discussed previously in [GigaSMART GTP Whitelisting and GTP Flow Sampling](#). As is the case with regular non-overlap GTP mapping, GTP forward listing selects specific subscribers based on IMSI, whereas GTP flow sampling uses map rules to select subscribers and then forward a percentage of the packets to tool ports.

## Configuration Considerations

This section details certain configuration considerations that apply only to the configuration of GTP forward listing and flow sampling maps for GTP overlap flow sampling maps.

### About GTP Overlap Flow Sampling Map Mode and Port Groups

A second level type map specifying GTP overlap flow sampling map mode must be selected to configure GTP forward listing and flow sampling maps.

To configure a GTP whilelisting map in overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Whitelisting Overlap** in a map.

To configure a GTP flow sampling map in GTP overlap flow sampling map mode, select **Type** as **Second Level** and **Subtype** as **Flow Sample Overlap** in a map .

You can configure one GTP forward listing map and one GTP flow sampling map pair that contain traffic policies corresponding to one destination port group. The load balanced port groups can contain a single port, a port range, or a GigaStream. Note that, starting in software version 4.8, port groups used in GTP overlapping maps support GigaStream.

The maximum number of port groups per single GTP overlap flow sampling map group is six.

For more information about port groups, refer to [Port Groups](#).

## Maximum Number of Port Group Members

The Maximum number of port group members can be determined as follows:

### Standalone Configuration

In a standalone configuration, use the following sequence :

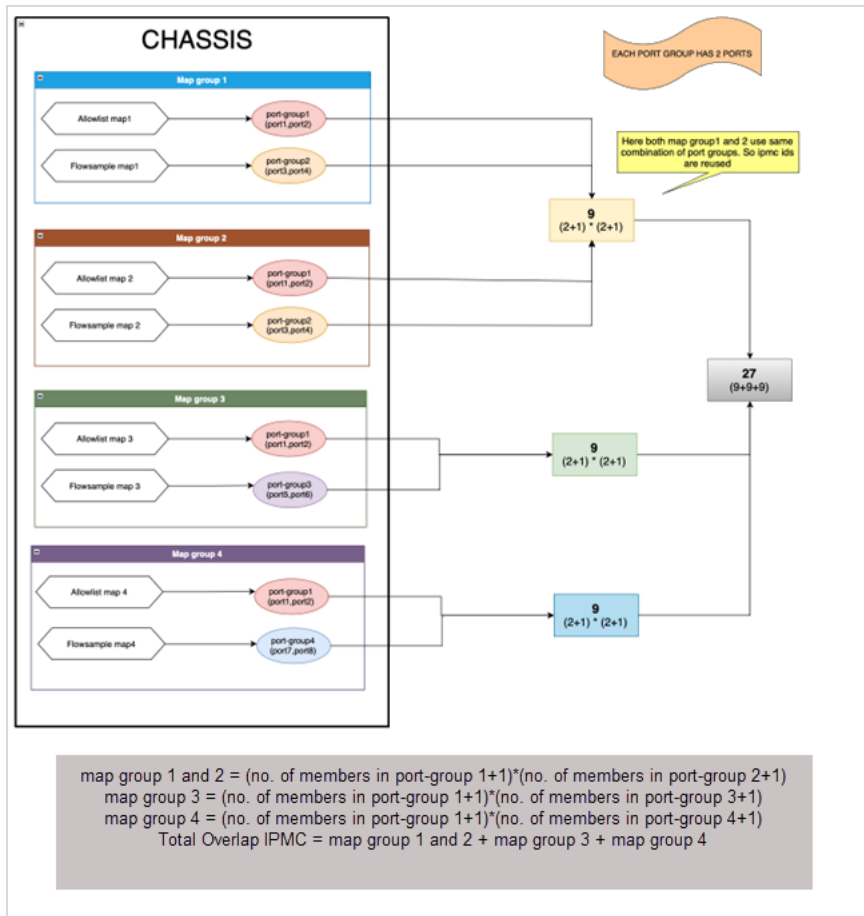
1. Determine the number of members per port group and add 1.
2. Multiply each port group result by each other.
3. The total multiplication should not exceed 4096.

For instance, assume the following configuration in a GTP overlap mapping group:

- o Port Group 1–2 load-balanced GigaStream
- o Port Group 2–3 load-balanced GigaStream
- o Port Group 3–1 load-balanced tool port
- o Port Group 4–1 load-balanced GigaStream
- o Port Group 5–4 load-balanced tool ports. The total number becomes:  $(2+1)*(3+1)*(1+1)*(1+1)*(4+1) = 240$

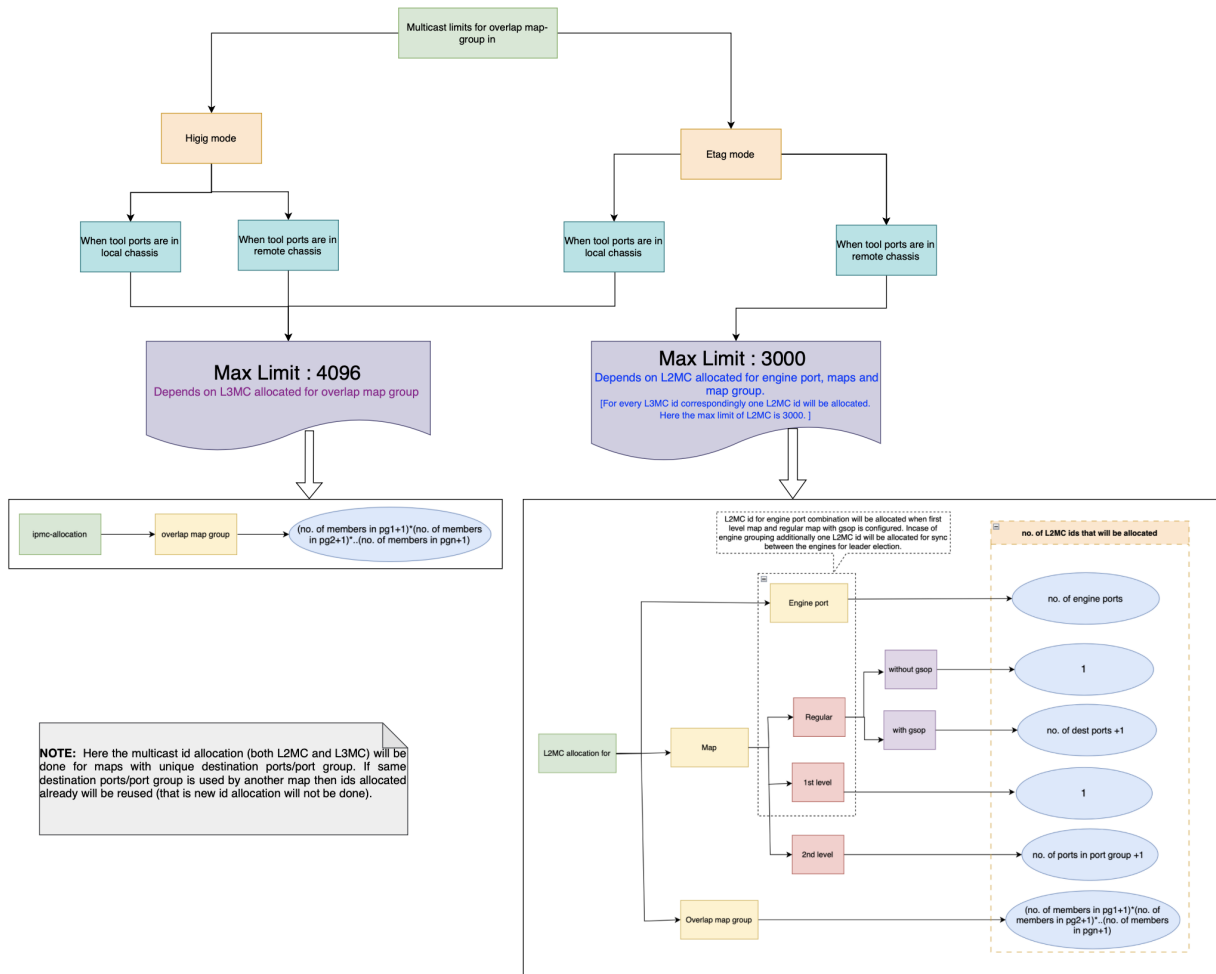
The tool configuration shown is accepted since this does not exceed the maximum number of multicast IDs (4096).

If Port Groups are utilized across multiple map groups in a single cluster, refer to the representation below on how the multicast IDs are calculated.



## Cluster Configuration

In a cluster configuration, Multicast IDs can defer based on Hi-Gig mode or E-tag mode. The below is representation of the same.



**NOTE:** The maximum Layer 2 multicast limit in E-tag cluster mode is 3000. It is recommended to keep the configured multicast entries within this limit. Current resource usage can be checked using command `show ipmc-resource`. If you encounter issues due to limit exhaustion, delete device configurations that exceed the limit and upgrade to the latest image or version. Prior to upgrading to the latest version/image, ensure that the maximum multicast limit is not exceeded.

## GTP Overlap Flow Sampling Map Priority

Since a packet matches multiple maps independently the concept of second level map priority does not apply to GTP overlap flow sampling maps. A GTP overlap flow sampling map pair consists of one GTP forward listing map and one GTP flow sampling map having the same destination port group. Within a GTP overlap flow sampling map pair the forward listing map rules will be applied before the flow

sampling map rules.

## Virtual Port Configuration in GTP Overlap Mode

In GTP Overlap map configuration, the virtual port sending traffic to all the port groups needs to be configured in GTP overlap mode.

To configure the virtual port with GTP overlap mode, select **GTP Overlap** when configuring the virtual port.

## About Map Groups

To create a group of maps for GTP forward listing and GTP flow sampling, select **Maps > Maps > Map Groups**, and then click **New**. The maps for a map group are entered in the **Maps** field. Refer to [Configuration Considerations](#). All the maps in a map group receive traffic according to map rules, rather than map priority. Thus, multiple copies of a GTP packet can be sent to more than one tool.

The **Maps** field of the Map Group page groups the forward listing and flow sampling maps. For example, assuming that two forward listing maps (**WLMAP1** and **WLMAP2**) and two flow sampling maps (**FSMAP1** and **FSMAP2**) have been configured in GTP overlap mode, the following example groups them all into the same map group called **map-group1**:

Keep in mind the following configuration considerations for map groups:

- A map group can be associated with only one GigaSMART group (gsgroup).
- All maps within a map group must be connected to the same vport.
- A map group can consist of only one GTP forward listing map or only one GTP flow sampling map but it cannot contain two maps of the same type.
- Once a map group is created, it cannot be edited to change the type or subtype of the map. However, you can add and edit the map rules for a map while it is configured in a map group.
- If multiple map groups are configured, the maps within each map group must point to the same port groups as the other map groups.

For more information about map groups, refer to [Create Map Groups](#).

## About Whitelist Maps

The GTP forward list is an IMSI list which is common to all forward list maps. You can configure an optional rule within a forward list map to specify a GTP version or interface-based policy.

Other than specifying a new second level type using **Type Second Level** and **Subtype Flow Whitelist Overlap** when creating the map, the configuration of GTP forward list maps follows the same configuration guidelines as given in the section [GTP Whitelisting](#).

A maximum of six forward list maps sending traffic to six different port groups can be configured per GigaSMART group (gsgroup).

## About Flow Sampling Maps

In GTP overlap flow sampling map mode, GTP flow sampling (rule-based flow sampling) is performed after GTP forward list-based forwarding. Therefore, flow sampling maps have a lower priority than forward list maps. Thus, within a GTP overlap map pair that consists of a single GTP forward list overlap map and a GTP flow sampling overlap map, the GTP forward list map is of higher priority.

Within the flow sampling maps, the rules in the first map have a higher priority than the rules in the second, third, and subsequent maps. Within any single map, rules are evaluated in order.

A maximum of six flow sampling maps sending traffic to six different port groups can be configured per GigaSMART group (gsgroup).

## Overlap Map Statistics

Starting with version 5.4 overlap and non-overlap maps are available. Overlap maps are displayed based on the following:

- If at least 1 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 1 pair of maps accepts the packets, the Sample (Tx) counters in the GTP Interface stats is incremented only once.
- If at least 1 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 1 pair of maps matches the packets, the Sample (Tx) counters in the GTP Interface stats is incremented only once.
- If there are no WL maps and all flow sample maps are no rule match, then Sample(Tx) and Sample Out counters in the GTP Interface stats is not incremented.

### GTP Overlap Flow Sampling Maps Example

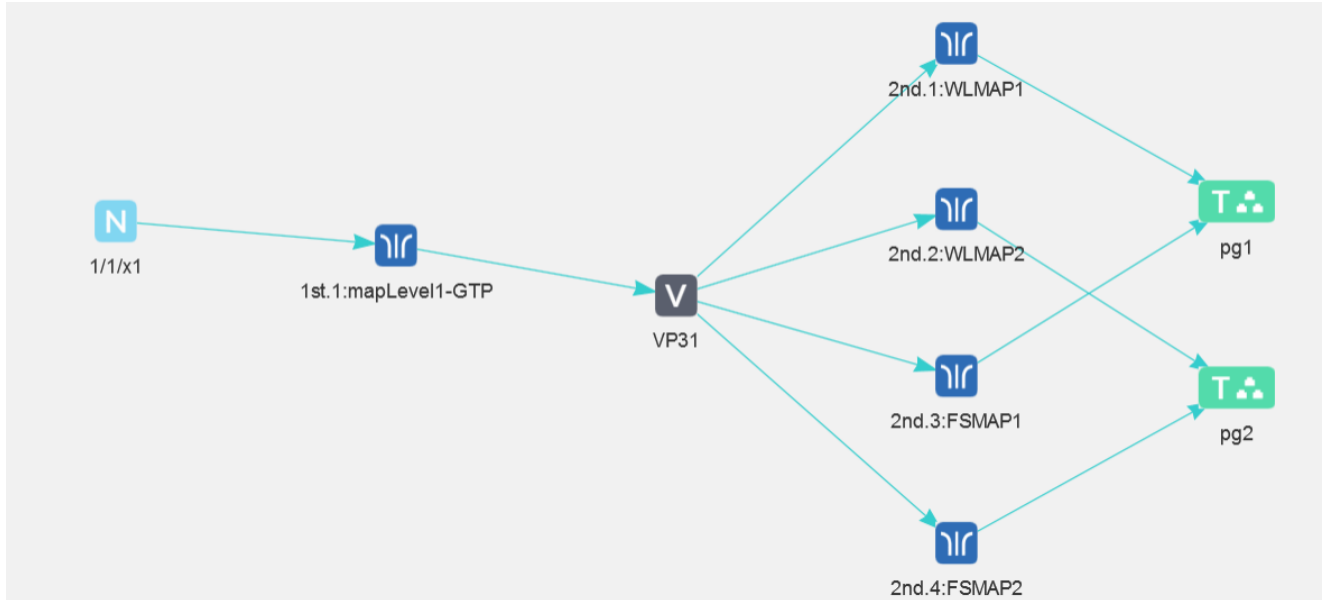
#### This section contains:

- [Example 1: GTP Overlap Mode](#)

### Example 1: GTP Overlap Mode

Example 1 is a GTP overlap mapping mode example.

In Example 1, traffic from a single network port goes to a single first level map (mapLevel1-GTP) which directs GTP-Control, and GTP-User traffic to a virtual port (VP31). Traffic from VP31 is replicated to two GTP whitelisting maps (WLMAP1 and WLMAP2) and two GTP flow sampling maps (FSMAP1 and FSMAP2), which then forward accepted traffic to the final port-group destinations, pg1 and pg2, for load balancing (refer to [Figure 27GTP Overlap Mode Example 1](#)).



**Figure 27** GTP Overlap Mode Example 1

**NOTE:** In Example 1, the tool ports and GigaStreams in the port group are on the same node as the GigaSMART group and GigaSMART operation.

Within each GTP whitelisting and flow sampling pair, if there is not a match to an IMSI in the whitelist map, the traffic flow is sampled based on the rules in the flow sampling map. The flow sampling rules specify IMSI, IMEI, and MSISDN numbers, as well as the percentage to sample.

Within each map pair, packets are then accepted or rejected. Accepted packets are forwarded to the port groups for load balancing. Rejected packets are dropped.

Use the following steps to configure example 1.

| Task | Description                                                                                                                          | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Create GigaStreams that will be part of the port groups                                                                              | <ol style="list-style-type: none"> <li>Select Ports &gt; Port Groups &gt; GigaStreams</li> <li>Click New.</li> <li>Enter gs1 in the Alias field.</li> <li>In the Ports field, select port 1/1x16 and 1/1x17.</li> <li>Click Save.</li> <li>Configure a second GigaStream with the alias gs2, select ports 1/1/x1 and 1/1/x2 in the Ports field, and click Save.</li> </ol>                                                                                                                                                                                |
| 2    | Create port groups and specify the tool ports and assign GigaStreams to the port groups. The port groups will also be load balanced. | <ol style="list-style-type: none"> <li>Select Ports &gt; Port Groups &gt; All Port Groups.</li> <li>Click New.</li> <li>Enter pg1 in the Alias field.</li> <li>Select Type GigaSMART Load Balancing.</li> <li>In the Ports field, select ports 1/1/x6 and 1/1/x7.</li> <li>In the GigaStream field, select gs1</li> <li>Click Save.</li> <li>Configure a second Port Group. with the alias pg2, select ports 1/1/x18 and 1/1/x10 in the Ports field, select GigaSMART Load Balancing, select pg2 in the GigaStream field, and then click Save.</li> </ol> |
| 3    | Configure a GigaSMART group and associate it with a GigaSMART engine port.                                                           | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; GigaSMART Groups.</li> <li>Click New.</li> <li>Enter GS31 in the Alias field.</li> <li>In the Port List field, select an engine port. For example 1/3/e1.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                              |
| 4.   | Create a virtual port.<br><b>Note:</b> You must enable GTP Overlap when configuring a virtual port for GTP overlap mapping.          | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; Virtual Ports &gt; Virtual Ports.</li> <li>Click New</li> <li>Enter VP31 in the Alias field.</li> <li>In the GigaSMART Group field, select GS31.</li> <li>Select GTP Overlap,</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                          |
| 5.   | Create the GTP Whitelist                                                                                                             | <ol style="list-style-type: none"> <li>From the device view, select GigaSMART &gt; GTP Whitelist.</li> <li>Click New.</li> <li>Enter Whitelist in the Alias field</li> </ol>                                                                                                                                                                                                                                                                                                                                                                              |

| Task | Description                                                                    | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                | d. Go to Task 6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 6.   | Fetch whitelist files from a specified location to populate the GTP whitelist. | a. On the GTP Whitelist page, select Bulk Upload.<br>b. Select Bulk Entry Operation for IMSI Upload Type<br>c. Select Upload from URL from the Bulk Upload Type list.<br>d. Enter the URL in the Enter Remote URL field. For example,<br>http://10.1.1.100/tftpboot/myfiles/MyIMSI_file2.tx<br>e. Click Save.                                                                                                                                                                                                                                                                                     |
| 7.   | Associate the GigaSMART group to the GTP whitelist.                            | a. From the device view, select GigaSMART > GigaSMART Groups > GigaSMART Groups<br>b. Select GS Group GS31 created in Task 3 and click Edit<br>c. Under GTP Whitelist, click on the GTP Whitelist Alias field and select Whitelist.<br>d. Click Save.                                                                                                                                                                                                                                                                                                                                             |
| 8.   | Configure the GigaSMART operation for GTP whitelisting.                        | a. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation.<br>b. Click New.<br>c. Enter gtp-overlapwhitelist1 in the Alias field.<br>d. Select the GigaSMART Group GS31 from the GigaSMART Groups list.<br>e. Select GTP Whitelist from the GigaSMART Operations (GSOP) list<br>f. Select Load Balancing from the GigaSMART Operations (GSOP) list.<br>g. Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>• Select Stateful</li> <li>• Set Type to GTP</li> <li>• Select Hashing</li> <li>• Select IMSI</li> </ul> h. Click Save. |
| 9.   | Configure the GigaSMART operation for GTP flow sampling.                       | a. From the device view, select GigaSMART > GigaSMART Operations (GSOP) > GigaSMART Operation.<br>b. Click New.<br>c. Enter gtp-overlapsampling1 in the Alias field.                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Task | Description                                                                                                                                                                                                                        | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                    | <ul style="list-style-type: none"> <li>d. Select the GigaSMART Group GS31 from the GigaSMART Groups list.</li> <li>e. Select Flow Sampling-GTP</li> <li>f. Select Load Balancing from the GigaSMART Operations (GSOP) list.</li> <li>g. Configure Load Balancing as follows: <ul style="list-style-type: none"> <li>• Select Stateful</li> <li>• Set Type to GTP</li> <li>• Select Hashing</li> <li>• Select IMSI</li> </ul> </li> <li>h. Click Save.</li> </ul> |
| 10.  | Configure the first level maps.<br>In the rules, 2123 is GTP-c traffic and 2152 is GTP-u traffic.                                                                                                                                  | <ul style="list-style-type: none"> <li>a. Configure the first map as follows: <ul style="list-style-type: none"> <li>• Alias: mapLevel1-GTP</li> <li>• Type and Subtype: First Level By Rule</li> <li>• Source: 1/1/x1</li> <li>• Destination: VP31</li> <li>• Rule 1: Pass, Bi Directional, Port Destination 2123</li> <li>• Rule 2: Pass, Bi Directional, Port Destination 2152</li> <li>• Click Save.</li> </ul> </li> </ul>                                  |
| 11.  | Configure the first second level GTP overlap map for GTP whitelisting. If there is a match to an IMSI in the whitelist for GTP version 1 traffic, it is then forwarded to load balancing port group <i>pg1</i> .                   | <ul style="list-style-type: none"> <li>a. Select Maps &gt; Maps &gt; Maps.</li> <li>b. Click New</li> <li>c. Configure the map. <ul style="list-style-type: none"> <li>• Alias: WLMAP1</li> <li>• Type and Subtype: Second Level GTP Flow Whitelist Overlap</li> <li>• Source: VP3</li> <li>• Destination: pg1</li> <li>• GSOP: gtp-whitelist</li> <li>• Rule 1: GTP, APN: Version V1</li> </ul> </li> <li>d. Click Save.</li> </ul>                             |
| 12.  | Configure a second level map for GTP flow sampling, the flow sampling map. If there is not a match to an IMSI in the whitelist, the traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to load | <ul style="list-style-type: none"> <li>a. Select Maps &gt; Maps &gt; Maps.</li> <li>b. Click New</li> <li>c. Configure the map. <ul style="list-style-type: none"> <li>• Alias: FSMAP1</li> </ul> </li> </ul>                                                                                                                                                                                                                                                    |

| Task | Description                                                                                                                                                                                                                                                                                                               | UI Steps                                                                                                                                                                                                                                                                                                                                                                    |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | balancing port group <i>pg1</i> .                                                                                                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>Type and Subtype: Second Level GTP Flow Sample Overlap</li> <li>Source: VP3</li> <li>Destination: pg1</li> <li>GSOP: gtp-overlapsample1</li> <li>Rule 1: GTP, IMSI: 3102609834*, IMEI: 35609506*, Percentage: 20</li> </ul> <p>d. Click Save.</p>                                                                                    |
| 13.  | Configure the next second level GTP overlap map for GTP whitelisting. If there is a match to an IMSI in the whitelist for GTP version 2 traffic, it is then forwarded to load balancing port group <i>pg2</i> .                                                                                                           | <p>a. Select Maps &gt; Maps &gt; Maps.</p> <p>b. Click New.</p> <p>c. Configure the map.</p> <ul style="list-style-type: none"> <li>Alias: WLMAP2</li> <li>Type and Subtype: Second Level Flow Whitelist Overlap</li> <li>Source: VP31</li> <li>Destination: pg2</li> <li>GSOP: gtp-whitelist</li> <li>Rule 1: GTP, APN: Version V2</li> </ul> <p>d. Click Save.</p>        |
| 14.  | Configure the next second level map for GTP flow sampling. If there is not a match to an IMSI in the whitelist as evaluated by the second level GTP whitelisting map <i>WLMAP2</i> , the traffic flow is sampled based on the rules in this map. Accepted packets are forwarded to load balancing port group <i>pg2</i> . | <p>a. Select Maps &gt; Maps &gt; Maps.</p> <p>b. Click New.</p> <p>c. Configure the map:</p> <ul style="list-style-type: none"> <li>Alias: FSMAP2</li> <li>Type and Subtype: Second Level GTP Flow Sample Overlap</li> <li>Source: VP31</li> <li>Destination: pg2</li> <li>Rule 1: GTP, IMSI: 3102609835*, IMEI: 35609507*, Percentage: 20</li> </ul> <p>d. Click Save.</p> |
| 15.  | Configure a map group. Add the GTP whitelisting and the two GTP flow sampling maps configured in previous steps.                                                                                                                                                                                                          | <p>a. Select Maps &gt; Map Groups.</p> <p>b. Click New.</p> <p>c. Enter OverlapMap in the Alias field.</p> <p>d. In the Maps field, select WLMAP1,WLMAP2,FSMAP1,FSMAP2.</p> <p>e. Click Save.</p>                                                                                                                                                                           |

## GTP Stateful Session Recovery

### Required License: GTP Filtering & Correlation

GTP sessions can be backed up periodically so they can then be recovered faster after a GigaSMART line card reboot or a node reboot. GTP stateful session recovery provides session persistence for GigaSMART GTP applications, including GTP flow filtering, GTP forward listing, and GTP flow sampling.

GTP stateful session recovery requires additional memory for storing backups. GigaVUE-HC3 has the required memory.

Using GTP stateful session recovery, the GTP session tables in the GigaSMART line card memory will be periodically backed up to the control card memory on the node and stored.

You can configure an interval for how often the backups occur, such as every 10 minutes. If GTP stateful session recovery is enabled and the GigaSMART line card is rebooted, the GTP session tables will be restored automatically following the reboot.

The last stored backup file will be downloaded from the control card to the GigaSMART line card using FTP. The session table will be repopulated from the last stored backup file to each GigaSMART engine, up to 8 engines. Packet count statistics for sessions are saved and will also be restored.

Depending on the size of the session table, the amount of time to restore from the backup might take as much as 3 minutes. During that interval, traffic will be blocked to the virtual port on the GigaSMART line card. Once the session table is read and populated, traffic will be allowed.

Depending on the interval between backups, there could be differences between the stored state and the current state of the system, for example, map configuration could change, or sessions could be added, modified, or deleted.

Load balancing information is not persisted, so after a session table is repopulated, a session that was once sent to one load balanced port may be sent to a different load balanced port after the reboot. However, for IMSI-based load balancing, the traffic might be sent to the same port as it was before the reboot.

GTP stateful session recovery works in a cluster environment; however, the cluster leader must remain the same.

To enable **GTP Session Recovery**, the system must retain specific session information. This is where **GTP Persistence** comes in. It allows us to define how long session data is stored and how the application should handle session continuity across interruptions.

Configure GTP Persistence

To enable GTP persistence, as well as to configure timers, use the GTP Persistence fields under GigaSMART Parameters on the GigaSMART Group configuration page shown in [Figure 28GTP Persistence GigaSMART Parameters](#) and select **GTP Persistence**. The timers are preconfigured with default values.

▼ GTP Persistence

GTP Persistence

☒

GTP Persistence Interval (minutes)

10

GTP Persistence Restart Age Time (minutes)

30

GTP Persistence File Age Timeout (minutes)

30

Figure 28 GTP Persistence GigaSMART Parameters

Use the **System** widget on the Overview page to determine the amount of memory. The size of memory will be 24Gb in an upgraded system. To view the System information, select **Overview** from the Navigation pane. The amount of free and used memory is displayed in the **Memory** field.

To see backup and restore information for GTP Persistence, select **GigaSMART > GigaSMART Groups > GigaSMART Groups**, and then click on the alias of the GigaSMART group. A Quick View opens for the selected GigaSMART group. Scroll down do GTP Persistence. In [Figure 29GTP Persistence Information](#), GigaSMART Group gsggrp-1\_4\_e1 is selected and the Quick View displayed.

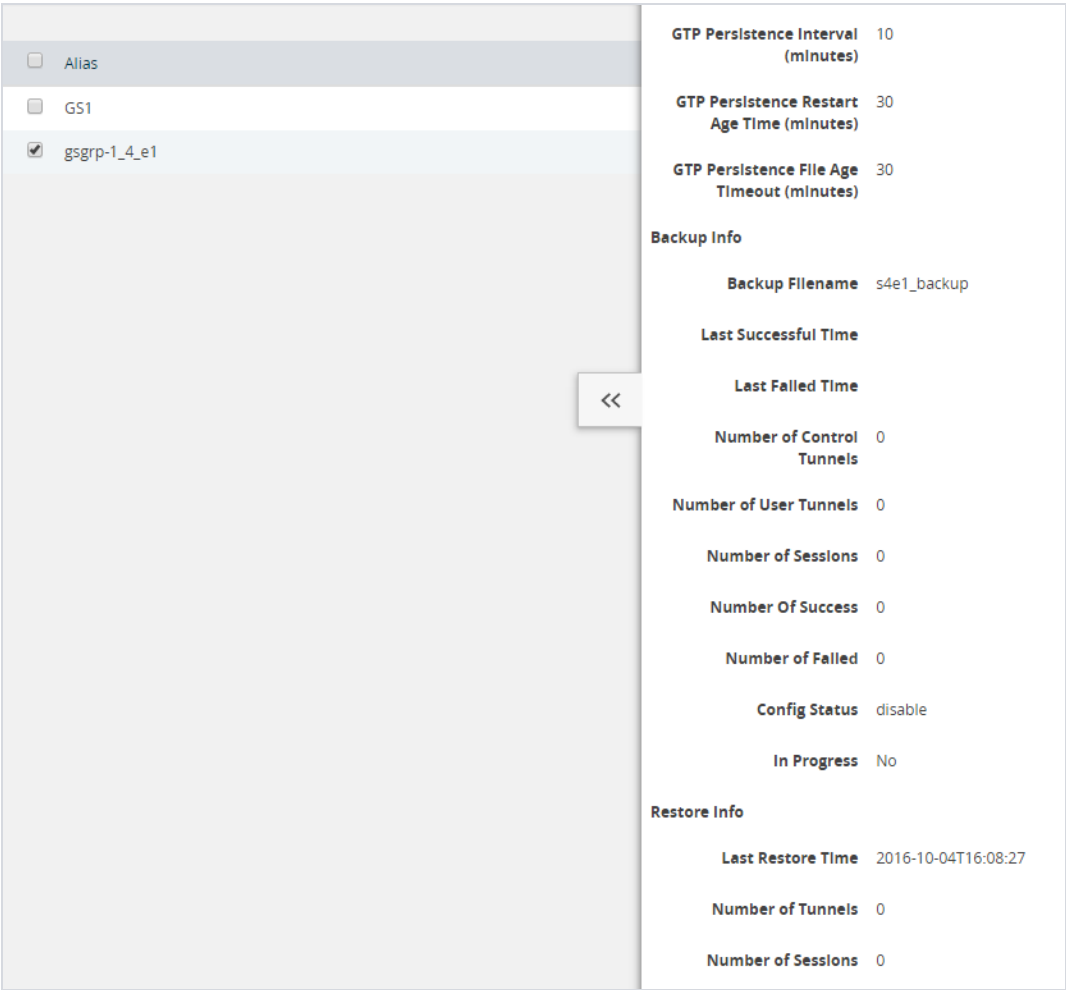


Figure 29 GTP Persistence Information

The following table describes persistence information.

Table 5: GigaSMART GTP Persistence Information

| Name                      | Format                                                            |
|---------------------------|-------------------------------------------------------------------|
| Backup Info               |                                                                   |
| Backup filename           | The internal name of the backup file.                             |
| Last successful time      | The timestamp of the last successful backup.                      |
| Last fail time            | The timestamp of the last failed backup.                          |
| Number of control tunnels | The number of control tunnels backed up.                          |
| Number of user tunnels    | The number of user tunnels backed up.                             |
| Number of sessions        | The number of sessions backed up.                                 |
| Number of success         | The number of successful backups.                                 |
| Number of failed          | The number of failed backups.                                     |
| Config Status             | The status of a backup, which will be either Enabled or Disabled. |

| Name                | Format                                        |
|---------------------|-----------------------------------------------|
| In Progress         | The progress, which will be either Yes or No. |
| <b>Restore Info</b> |                                               |
| Last restore time   | The timestamp of the last restore.            |
| Number of tunnels   | The number of tunnels restored.               |
| Number of sessions  | The number of sessions restored.              |

To delete backup files, select the alias of GigaSMART Group and click **Edit**. Scroll down to GTP Persistence (refer to [Figure 30 GTP Backup Files Delete](#)) and click **Delete All** under **GTP Backup Files**.

The screenshot shows a configuration window for GTP Persistence. At the top, there's a header 'GTP Persistence' with a dropdown arrow. Below it, there's a checkbox labeled 'GTP Persistence'. Underneath, there are three rows, each with a label and a value: 'GTP Persistence Interval (minutes)' with value '10', 'GTP Persistence Restart Age Time (minutes)' with value '30', and 'GTP Persistence File Age Timeout (minutes)' with value '30'. At the bottom, there's a section labeled 'GTP Backup Files' which contains a button labeled 'Delete All'. A mouse cursor is pointing at the 'Delete All' button.

**Figure 30** GTP Backup Files Delete

Refer to *GigaSMART GTP Stateful Session Recovery* in the GigaVUE-OS CLI Reference Guide.

## GTP Scaling

GTP can be scaled as follows:

- [GigaSMART Cards in GigaVUE-OS Devices](#)
- [GTP Engine Grouping](#)

### GigaSMART Cards in GigaVUE-OS Devices

#### Required License: GTP Filtering & Correlation

A total of four GigaSMART SMT-HC3-C08 line cards are supported on a single GigaVUE-HC3 node. This provides a total of eight GigaSMART engine ports, which increases the amount of GigaSMART processing available on the GigaVUE-HC3.

The increased number of GigaSMART line cards in the GigaVUE-HC3 can be used by the following GTP applications: GTP flow filtering, GTP flow sampling, and GTP whitelisting.

## GTP Engine Grouping

## Required License: GTP Filtering &amp; Correlation

A GigaSMART group (gsgroup) associated with GTP applications can have multiple GigaSMART engine port members. You can combine up to eight engine ports to form an engine group. The engine group provides higher capacity to GTP applications by load balancing GTP user-data plane (GTP-u) traffic among the members of the group. Grouping multiple GigaSMART engine ports increases the effective throughput for GTP applications.

**NOTE:** A GigaSMART Engine Group supports supports 12 million GTP subscriber sessions for GigaVUE HC3 nodes.

GTP engine grouping is supported on GigaVUE-HC3 nodes.

GTP engine grouping can be used by the following GTP applications: GTP flow filtering, GTP flow sampling, and GTP whitelisting.

The following table lists GTP engine grouping support for GigaVUE-FM,GigaVUE HC Series nodes:

| GigaVUE-FM,GigaVUE HC Series Node | Maximum Number of GigaSMART Line Cards per Node | Number of e ports per Line Card | Supported Number of e ports per GigaSMART Group | Location of e ports      |
|-----------------------------------|-------------------------------------------------|---------------------------------|-------------------------------------------------|--------------------------|
| GigaVUE-HC3                       | 4                                               | 2                               | 8                                               | e1 and e2 on same module |
| GigaVUE-HC1                       | Not supported in this software version.         |                                 |                                                 |                          |

Keep in mind the following recommendations and restrictions:

- Configure a GTP engine group on a single GigaVUE-FM,GigaVUE HC Series node.
- GTP engine grouping only supports IMSI hash-based load balancing.
- GTP engine grouping is limited to out-of-band cluster configurations in this software version.

## Passing GTP Control Traffic

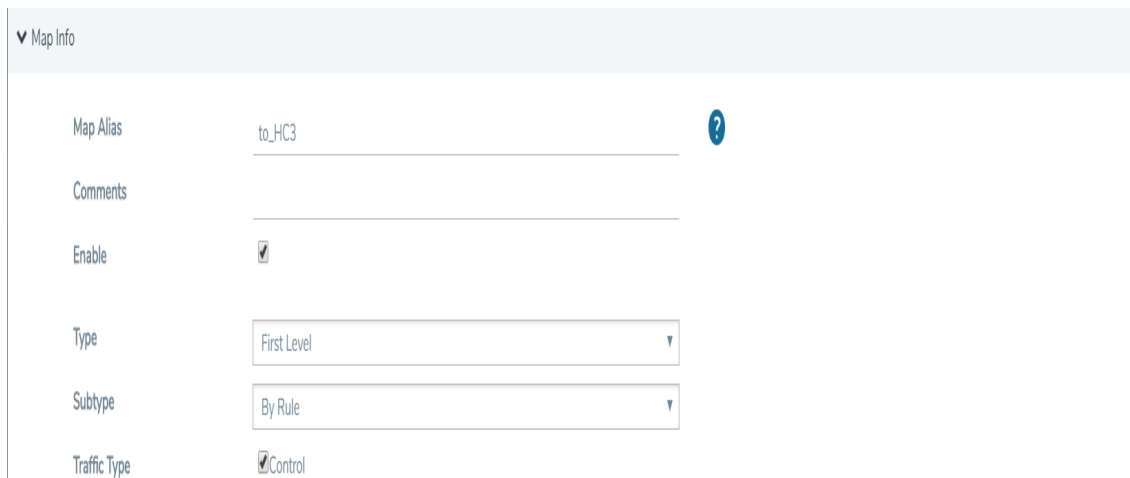
Enable the **ControlTraffic** checkbox when creating a First Level By Rule map, to allow GTP applications to pass GTP control traffic (GTP-c) to all GigaSMART engines in a GTP engine group. GTP-c traffic is sent to all members of the engine group in order to replicate the session tables.

**NOTE:** In the map with the **ControlTraffic** enabled, only one vport is supported.

You can edit the map with **ControlTraffic** option enabled. For example, **Control Traffic** can be selected in an existing first level map, or it can be deleted from a first level map. Other editing, such as changing the **Source** or the **Destination** in the first level map is also allowed.

To set GTP Control Traffic:

1. From the device view, select **GigaSMART > Maps > Maps** and click **New**.
2. On the New Map page, select **First Level** and **By Rule** for the map type and subtype, respectively.
3. Enable **Control Traffic** as shown in the following figure.
4. Configure the map and click **Save** when done.



The screenshot shows the 'Map Info' configuration page. It includes the following fields and values:

| Field        | Value                                       |
|--------------|---------------------------------------------|
| Map Alias    | to_HC3                                      |
| Comments     |                                             |
| Enable       | <input checked="" type="checkbox"/>         |
| Type         | First Level                                 |
| Subtype      | By Rule                                     |
| Traffic Type | <input checked="" type="checkbox"/> Control |

## Upgrade from Earlier Release

When there is existing GTP configuration with one engine port per GigaSMART group in an earlier software version, an upgrade from that earlier software version to a higher release will succeed.

However you cannot convert that configuration to multiple engine ports per GigaSMART group. You must delete the configuration and reconfigure it, including the GigaSMART group, GigaSMART operation, virtual port, and maps. This is due to the need for separate maps for GTP control plane and GTP user plane traffic in higher releases.

## Modify Engine Ports in GigaSMART Group

You can modify the engine ports in a GigaSMART group. For example, you can add an engine port to a GigaSMART group or remove an engine port from a GigaSMART group. After the change, reset all the GigaSMART line cards or modules that have engine ports configured in the GigaSMART group.

## Modify vports in Map

You can modify the vport relating to the first level map with Control Traffic enabled. For example, you can change the vport configured in the map. After the change, reset all the GigaSMART line cards or modules that have engine ports configured in the vport.

### Configure GTP Engine Grouping

Refer to the following examples:

- [Required License: GTP Filtering & Correlation](#)
- [Required License: GTP Filtering & Correlation](#)

### Display Statistics

To display the GigaSMART Group statistics, select **GigaSMART > GigaSMART Groups > Statistics**.

Refer to [GigaSMART Group Statistics Definitions](#) for descriptions of the statistics.

### GTP Engine Grouping Configuration Examples

To configure GTP Engine Grouping refer to the following examples:

- [GTP Engine Grouping Configuration Example](#)
- [GTP Engine Grouping Configuration Complex Example](#)

## GTP Engine Grouping Configuration Example

This is an example of a GTP engine group consisting of two engine ports on a GigaVUE-HC1 node. This example includes a GigaSMART operation for GTP flow filtering.

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | UI Steps                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Configure ports as follows: <ul style="list-style-type: none"> <li>o one network type of port. This will be used as the <b>Source</b> attribute in two first level maps in <b>Task 5</b> and <b>Task 6</b>.</li> <li>o one tool type of port for the <b>Destination</b> attribute in a second level flow filtering map in <b>Task 7</b>.</li> <li>o one tool type of port for the <b>Destination</b> attribute in a shared collector map in <b>Task 8</b>.</li> </ul> Then administratively enable the ports. | <ol style="list-style-type: none"> <li>1. Select Ports &gt; Ports &gt; All Ports</li> <li>2. Click Quick Port Editor</li> <li>3. Configure a network port and two tool ports. For example, select Network for port 22/3/c1 and select Tool for ports 22/3/c2 and 22/1/c3.</li> <li>4. Select Enable for each port.</li> <li>5. Click OK.</li> <li>6. Close the Quick Port Editor.</li> </ol> |
| 2    | Configure a GigaSMART group and associate it with two GigaSMART engine                                                                                                                                                                                                                                                                                                                                                                                                                                        | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups.</li> </ol>                                                                                                                                                                                                                                                     |

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | port, to form the GTP engine group.<br>The GigaSMART group will be used in <b>Task 5</b> and <b>Task 6</b> .                                                                                                                                                                                                                                                                                                                                                                                                                     | <ol style="list-style-type: none"> <li>2. Type gsg2 in the Alias field.</li> <li>3. Click in the Port List field to add the two engine ports.</li> <li>4. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 3    | For GTP flow filtering, configure a flow filtering GigaSMART operation and assign it to the GigaSMART group. The gsop will be used in the second level flow filtering map in <b>Task 7</b> .                                                                                                                                                                                                                                                                                                                                     | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>2. Type gtp_gsg2 in the Alias field.</li> <li>3. Select gsg2 from the GigaSMART Groups list.</li> <li>4. Select Flow Filtering from the GigaSMART Operations list. (GSOP).</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                              |
| 4    | Configure a virtual port and assign it to the same GigaSMART group. This virtual port will be used as the <b>Destination</b> in the first level maps in <b>Task 5</b> and <b>Task 6</b> , as the <b>Source</b> in the second level map in <b>Task 7</b> , and as the <b>Source</b> attribute in the shared collector map in <b>Task 8</b> .                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; Virtual Ports.</li> <li>2. Click New.</li> <li>3. Type vp1 in the Alias field.</li> <li>4. Select gsg2 from the GigaSMART Groups list.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 5    | <p>Create a first level map that directs GTP control traffic from the physical network port to the virtual port created in <b>Task 4</b>.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <b>NOTE:</b> In the rule, 2123 is GTP-c traffic.         </div> <p>This map, with the <b>Control Traffic</b> attribute, identifies the GTP-c control traffic needed for GTP engine grouping.</p> <p><b>Note:</b> The order of configuration is important. Set <b>Control Traffic</b> before any map rules.</p> | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map.             <ul style="list-style-type: none"> <li>■ Type gtp_to_vp1-c in the Alias field</li> <li>■ Select First Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Enable Control Traffic</li> <li>■ Select 22/3/c1 for Source</li> <li>■ Select vp1 for Destination</li> </ul> </li> <li>4. Add a rule.             <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass and Bi Directional</li> <li>c. Select Port Destination and specify 2123</li> </ol> </li> <li>4. Click Save.</li> </ol> |
| 6    | <p>Create another first level map that directs GTP user traffic from the physical network port to the virtual port created in <b>Task 5</b>.</p> <p><b>Note:</b> In the rule, 2152 is GTP-u traffic.</p> <p>GTP-u traffic corresponding to the same GTP-c traffic will be sent to the same virtual port.</p>                                                                                                                                                                                                                     | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map.             <ul style="list-style-type: none"> <li>■ Type gtp_to_vp1 in the Alias field</li> <li>■ Select First Level for Type</li> <li>■ Select By Rule for Subtype</li> <li>■ Enable Control Traffic</li> <li>■ Select the network configured in Task 1 for Source</li> <li>■ Select vp1 for Destination</li> </ul> </li> <li>4. Add a rule.</li> </ol>                                                                                                                                                                                      |

| Task | Description                                                                                                                                                                                                                                 | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                             | <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass and Bi Directional</li> <li>c. Select Port Destination and specify 2123</li> <li>4. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 7    | Create a second level map for GTP flow filtering that takes traffic from the virtual port, applies the flow filtering GigaSMART operation, matches IMEIs and version specified by the flow rule, and sends matching traffic to a tool port. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Type from_vp1 in the Alias field.</li> <li>4. Configure the map. <ul style="list-style-type: none"> <li>■ Select Second Level for Type</li> <li>■ Select Flow Filter for Subtype</li> <li>■ Select vp1 for Source</li> <li>■ Select one of the tool ports configured in Task 1 for Destination.</li> <li>■ Select gtp_gsg2 for from the GSOP list.</li> </ul> </li> <li>5. Add a Rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select GTP IMEI.</li> <li>d. Specify * in the IMEI field.</li> <li>e. Select V2 for Version.</li> </ol> </li> <li>6. Click Save.</li> </ol> |
| 8    | Add a shared collector for any unmatched traffic from the virtual port and send it to a different tool port than in <b>Task 7</b> .                                                                                                         | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Click New.</li> <li>3. Configure the map. <ul style="list-style-type: none"> <li>■ Type from_vp1_scoll in the Alias field.</li> <li>■ Select Second Level for Type</li> <li>■ Select Collector for Subtype</li> <li>■ Select vp1 for Source.</li> <li>■ Select the other tool port configured in Task 1 for Destination.</li> </ul> </li> <li>4. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                    |

## GTP Engine Grouping Configuration Complex Example

This is a more complex example of GTP engine grouping than the previous example. This example has four engine ports on two GigaSMART line cards on the same GigaVUE-HC3 node. The GigaSMART line cards are in slots 1 and 3.

The GigaVUE-HC3 node is the cluster leader of a two-node out-of-band cluster. A GigaVUE-HC1 is the standby node in the cluster.

This example includes GigaSMART operations for GTP flow filtering with load balancing, GTP flow sampling with load balancing, and GTP whitelisting. The forward list must be associated with the GigaSMART group on the leader, the GigaVUE-HC3.

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <p>Configure ports on the GigaVUE-HC3 as follows:</p> <ul style="list-style-type: none"> <li>One network type of port. This will be used as the <b>Source</b> attribute in two first level maps in <b>Task 11</b> and <b>Task 12</b>.</li> <li>Twelve tool type of ports. There are four tool ports in each of three port groups used for load balancing. The port groups will be created in <b>Task 6</b>.</li> <li>Five tool type of ports for a GigaStream that will be created in <b>Task 2</b>.</li> <li>Two tool type of ports for another GigaStream that will be created in <b>Task 2</b>.</li> </ul> <p>Then administratively enable the ports.</p> | <ol style="list-style-type: none"> <li>On the GigaVUE-HC3, select Ports &gt; Ports &gt; All Ports</li> <li>Click Quick Port Editor.</li> <li>Configure one network port for <b>Task 11</b> and <b>Task 12</b>. For example, 23/2/c3.</li> <li>Configure 12 tool ports for three port groups in <b>Task 6</b>. For example, 23/3/x1..x4 for the first port group, 23/3/x9..x12 for the second tool group, and 23/3/x13..x16 for the third port group.</li> <li>Configure five tool ports for a GigaStream in <b>Task 2</b>. For example, 23/3/x20..x24.</li> <li>Configure two tool ports for another GigaStream in <b>Task 2</b>. For example, 23/2/c1..c2 type tool.</li> <li>Select enable for each port.</li> <li>Click OK.</li> <li>Close the Quick Port Editor.</li> </ol> |
| 2    | <p>On the GigaVUE-HC3, configure one GigaStream using five tool ports. This will be used as the <b>Destination</b> attribute in the map in <b>Task 11</b>.</p> <p>Configure another GigaStream to be used in the stack link between the GigaVUE-HC3 and GigaVUE-HC1 that will be created in <b>Task 4</b>.</p>                                                                                                                                                                                                                                                                                                                                               | <ol style="list-style-type: none"> <li>Select Ports &gt; Port Groups &gt; GigaStreams</li> <li>Configure a GigaStream with five tool ports. <ol style="list-style-type: none"> <li>Click New.</li> <li>Type hc3-gs-1 in the Alias field.</li> <li>Select Tool GigaStream.</li> <li>Click in the Ports field and select the five tool ports configured in Task 1.</li> <li>Click Advanced Hash Settings and use the Default setting.</li> <li>Click Save.</li> </ol> </li> <li>Configure another GigaStream with two tool ports. <ol style="list-style-type: none"> <li>Click New.</li> <li>Type hc3-80g in the Alias field.</li> <li>Select Tool GigaStream.</li> <li>Click in the Ports field and select the two tool ports</li> </ol> </li> </ol>                             |

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                                                           | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>configured in Task 1.</p> <ol style="list-style-type: none"> <li>Click Advanced Hash Settings and use the Default setting.</li> <li>Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 3    | <p>Configure ports on the GigaVUE-HC1 as follows:</p> <ul style="list-style-type: none"> <li>Two tool type of ports for a GigaStream that will be created in <b>Task 4</b>.</li> <li>One tool type of port that will be used as the <b>Destination</b> in a map in <b>Task 11</b>.</li> <li>Four tool type of ports for a GigaStream that will be created in <b>Task 4</b>.</li> </ul> <p>Then administratively enable the ports.</p> | <ol style="list-style-type: none"> <li>On the GigaVUE-HC1, select Ports &gt; Ports &gt; All Ports</li> <li>Click Quick Port Editor.</li> <li>Configure two tool ports for a GigaStream in <b>Task 4</b>. For example, 33/2/q1..q2</li> <li>Configure one tool ports for the map in <b>Task 11</b>. For example, 33/3/x11.</li> <li>Configure four tool ports for a GigaStream in <b>Task 4</b>. For example, 33/2/x20..x24.</li> <li>Select Enable for each port.</li> <li>Click OK.</li> <li>Close the Quick Port Editor.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                   |
| 4    | <p>On the GigaVUE-HC1, configure a GigaStream using two tool ports. This will be used in the stack link created in <b>Task 5</b>.</p> <p>Configure another GigaStream using four tool ports. This will be used in the shared collector in <b>Task 17</b>.</p>                                                                                                                                                                         | <ol style="list-style-type: none"> <li>Select Ports &gt; Port Groups &gt; GigaStreams</li> <li>Configure a GigaStream with five tool ports. <ol style="list-style-type: none"> <li>Click New.</li> <li>Type hc3-gs-4 in the Alias field.</li> <li>Select Tool GigaStream.</li> <li>Click in the Ports field and select the five tool ports configured in Task 1. For example, 33/2/x20..x25.</li> <li>Click Advanced Hash Settings and use the Default setting.</li> <li>Click Save.</li> </ol> </li> <li>Configure another GigaStream with two tool ports. <ol style="list-style-type: none"> <li>Click New.</li> <li>Type hc3-80g in the Alias field.</li> <li>Select Tool GigaStream.</li> <li>Click in the Ports field and select the two tool ports configured in Task 1. For example, 33/2/q1..q2.</li> <li>Click Advanced Hash Settings and use the Default setting.</li> <li>Click Save.</li> </ol> </li> </ol> |
| 5    | Configure the stack link between the GigaVUE-HC1 and GigaVUE-HC3.                                                                                                                                                                                                                                                                                                                                                                     | <ol style="list-style-type: none"> <li>Select Ports &gt; Port Groups &gt; Stack Links</li> <li>Click New.</li> <li>Select Stack GigaStream.</li> <li>For First Member select hc3-80g.</li> <li>For Second Member select hc3-80g</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 6    | Create three port groups and specify four tool ports each, for load balancing. Also,                                                                                                                                                                                                                                                                                                                                                  | <ol style="list-style-type: none"> <li>Select Ports &gt; Port Groups &gt; All Port Groups.</li> <li>Create the first port group.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                                      | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>enable load balancing on each port group.</p> <p>The port groups, hc3-pg-1 and hc3-pg-2, will be used as the <b>Destination</b> in two second level flow sampling maps in <b>Task 14</b> and <b>Task 15</b>.</p> <p>The port group, hc3-q2x32-1-4, will be used as the <b>Destination</b> in a second level flow filtering map in <b>Task 16</b></p>                                                          | <ol style="list-style-type: none"> <li>a. Click New.</li> <li>b. Type hc3-pg-1 in the Alias field.</li> <li>c. Select SMART Load Balancing.</li> <li>d. Click in the Ports field and select four tool ports. For example, 23/4/x9..x12.</li> <li>e. Click Save.</li> </ol> <ol style="list-style-type: none"> <li>6. Create the second port group. <ol style="list-style-type: none"> <li>a. Click New.</li> <li>b. Type hc3-pg-1 in the Alias field.</li> <li>c. Select SMART Load Balancing.</li> <li>d. Click in the Ports field and select four tool ports. For example, 23/4/x13..x16</li> <li>e. Click Save.</li> </ol> </li> </ol> <ol style="list-style-type: none"> <li>6. Create the second port group. <ol style="list-style-type: none"> <li>a. Click New.</li> <li>b. Type hc3-q2x32-1-4 in the Alias field.</li> <li>c. Select SMART Load Balancing.</li> <li>d. Click in the Ports field and select four tool ports. For example, 23/4/x13..x16</li> <li>e. Click Save.</li> </ol> </li> </ol> |
| 7    | <p>Configure a GigaSMART group and associate it with four GigaSMART engine ports, two in slot 1 and two in slot 3, to form the GTP engine group.</p> <p>The GigaSMART group will be used in <b>Task 8</b>, <b>Task 9</b>, and <b>Task 10</b>.</p>                                                                                                                                                                | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups.</li> <li>2. Click New.</li> <li>3. Type hc3scale-4engines-slots1and3.</li> <li>4. Click in the Port List and select the engine ports. For example, 3/1/e1,23/1/e2,23/3/e1,23/3/e2.</li> </ol> <p>Go to <b>Task 8</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 8    | <p>Associate the GigaSMART group to an existing GTP forward list.</p> <p><b>Note:</b> The forward list is only supported on the cluster leader, which is the GigaVUE-HC3 in this example.</p>                                                                                                                                                                                                                    | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; GigaSMART Groups &gt; GigaSMART Groups.</li> <li>2. Under GTP Whitelist, select the alias of an existing forward list. For example, gtp-whitelist.</li> <li>3. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 9    | <p>For GTP flow filtering, configure a flow filtering GigaSMART operation, specify load balancing, and assign the GigaSMART operation to the GigaSMART group. The hc3-scale-ff-lb gsop will be used in the second level flow filtering map in <b>Task 16</b>.</p> <p>For GTP flow sampling, configure a flow sampling GigaSMART operation, specify load balancing, and assign the GigaSMART operation to the</p> | <ol style="list-style-type: none"> <li>1. Configure a Flow Filtering operation. <ol style="list-style-type: none"> <li>a. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>b. Click New.</li> <li>c. Type hc3-scale-ff-lb in the Alias field.</li> <li>d. Select hc3scale-4engines-slots1and3 from the GigaSMART Groups list.</li> <li>e. Select Flow Filtering from the GigaSMART Operations (GSOP) list.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                                                            | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>GigaSMART group. The hc3-scale-fs-lb gsop will be used in the two second level flow sampling maps in <b>Task 15</b> and <b>Task 16</b>.</p> <p>For GTP forward listing, configure a whitelisting GigaSMART operation, and assign the GigaSMART operation to the GigaSMART group. (This GigaSMART operation is not load balanced.) The hc3-scale-wl gsop will be used in the second level forward listing map in <b>Task 13</b>.</p> | <ol style="list-style-type: none"> <li>f. Click Save.</li> <li>7. Configure a Flow Sampling operation. <ol style="list-style-type: none"> <li>a. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>b. Click New.</li> <li>c. Type hc3-scale-fs-lb in the Alias field.</li> <li>d. Select hc3scale-4engines-slots1and3 from the GigaSMART Groups list.</li> <li>e. Select Flow Sampling from the GigaSMART Operations (GSOP) list.</li> <li>f. Select Flow Sampling -GTP</li> <li>g. Click Save.</li> </ol> </li> <li>8. Configure a Forward listing operation. <ol style="list-style-type: none"> <li>a. From the device view, select GigaSMART &gt; GigaSMART Operations (GSOP) &gt; GigaSMART Operation.</li> <li>b. Click New.</li> <li>c. Type hc3-scale-wl in the Alias field.</li> <li>d. Select hc3scale-4engines-slots1and3 from the GigaSMART Groups list.</li> <li>e. Select GTP Whitelist from the GigaSMART Operations (GSOP) list.</li> <li>f. Select Enabled (default).</li> <li>g. Click Save.</li> </ol> </li> </ol> |
| 10   | <p>Configure a virtual port and assign it to the same GigaSMART group. This virtual port will be used as the <b>Destination</b> in the first level maps in <b>Task 11</b> and <b>Task 12</b>, as the <b>Source</b> in the second level maps in <b>Task 13</b>, <b>Task 14</b>, <b>Task 15</b>, <b>Task 16</b>, and as the <b>Source</b> in the shared collector in <b>Task 17</b>.</p>                                                 | <ol style="list-style-type: none"> <li>1. From the device view, select GigaSMART &gt; Virtual Ports</li> <li>2. Click New.</li> <li>3. Type vp-hc3scale-4engines-slots1and3 in the Alias field.</li> <li>4. Select hc3scale-4engines-slots1and3 from the GigaSMART Groups list.</li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 11   | <p>Create a first level map that directs GTP control traffic from the physical network port to the virtual port created in <b>Task 10</b>.</p> <p><b>Note:</b> In the rule, 2123 is GTP-c traffic.</p> <p>This map, with the <b>Control Traffic</b> enabled, identifies the GTP-c control traffic needed for GTP engine grouping.</p> <p>In addition to the virtual port, traffic is also sent to a GigaStream and a tool port.</p>    | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map. <ul style="list-style-type: none"> <li>■ Type to_hc3_gtpc in the Alias field</li> <li>■ Select First Level for Type.</li> <li>■ Select By Rule for Subtype</li> <li>■ Enable Control Traffic</li> <li>■ Select a network port for the Source. For example, 23/3/q6.</li> <li>■ Select the GigaStream port hc3-gs-1, the virtual</li> </ul> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Task | Description                                                                                                                                                                                                                                                                                                   | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                                                                                                                                                                                                                               | <p>port p-hc3scale-4engines-slots1and3, and a tool port (for example, 23/7/q6) for the Destination.</p> <ol style="list-style-type: none"> <li>3. Add a rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass and Bi Directional.</li> <li>c. Select Port Destination for the rule.</li> <li>d. Enter 2123 for the port value.</li> </ol> </li> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 12   | <p>Create another first level map that directs GTP user traffic from the physical network port to the virtual port created in <b>Task 10</b>.</p> <p><b>Note:</b> In the rule, 2152 is GTP-u traffic.</p> <p>GTP-u traffic corresponding to the same GTP-c traffic will be sent to the same virtual port.</p> | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map. <ul style="list-style-type: none"> <li>■ Type to_hc3_gtpu_1 in the Alias field</li> <li>■ Select First Level for Type.</li> <li>■ Select By Rule for Subtype</li> <li>■ Select a network port for the Source. For example, 23/7/q6.</li> <li>■ Select the virtual port vp-hc3scale-4engines-slots1and3 for the Destination.</li> </ul> </li> <li>3. Add a rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass and Bi Directional.</li> <li>c. Select Port Destination for the rule.</li> <li>d. Enter 2152for the port value.</li> </ol> </li> <li>5. Add a second rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select Pass.</li> <li>c. Select IPv4 Fragmentation for the rule.</li> <li>d. Enter 2152for the port value.</li> <li>e. Select allFragNoFirst for Value.</li> </ol> </li> <li>6. Click Save.</li> </ol> |
| 13   | <p>Configure a second level map for GTP whitelisting, the forward list map, that takes traffic from the virtual port, applies the forward listing GigaSMART operation, and sends traffic to the remote GigaVUE-HC1 node through a GigaStream.</p>                                                             | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map. <ul style="list-style-type: none"> <li>■ Type from_hc3_wl in the Alias field</li> <li>■ Select Second Level for Type.</li> <li>■ Select By Rule for Subtype</li> <li>■ Select the virtual port vp-hc3scale-4engines-slots1and3 for the Source.</li> <li>■ Select the GigaStream hc3-gs-1 for the Destination.</li> <li>■ Select hc3-scale-wl from the GSOP list.</li> </ul> </li> <li>3. Click Save.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 14   | <p>Configure a second level map for GTP flow sampling. This is the first of two flow</p>                                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Task | Description                                                                                                                                                                                                                                                                                                                                                                                 | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>sampling maps.</p> <p>This map filters for version 2. It takes traffic from the virtual port and applies the flow sampling GigaSMART operation.</p> <p>Traffic flow is sampled based on the flow sampling rule in this map. Accepted packets are forwarded to load balancing port group hc3-pg-2.</p>                                                                                    | <ul style="list-style-type: none"> <li>■ Type from_hc3_fs_v2 in the Alias field</li> <li>■ Select Second Level for Type.</li> <li>■ Select Flow Sample for Subtype</li> <li>■ Select the virtual port vp-hc3scale-4engines-slots1and3 for the Source.</li> <li>■ Select the port group hc3-pg-2 for the Destination.</li> <li>■ Select hc3-scale-fs-lb from the GSOP list.</li> </ul> <ol style="list-style-type: none"> <li>3. Add a rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select GTP.</li> <li>c. Enter 60 for Percentage.</li> <li>d. Enter 5* in the IMSI field.</li> <li>e. Select V2 for Version</li> </ol> </li> <li>6. Click Save.</li> </ol>                                                                              |
| 15   | <p>Configure a second level map for GTP flow sampling. This is the second of two flow sampling maps.</p> <p>This map filters for version 1. It takes traffic from the virtual port and applies the flow sampling GigaSMART operation.</p> <p>Traffic flow is sampled based on the flow sampling rule in this map. Accepted packets are forwarded to load balancing port group hc3-pg-1.</p> | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map. <ul style="list-style-type: none"> <li>■ Type from_hc3_fs_v1 in the Alias field</li> <li>■ Select Second Level for Type.</li> <li>■ Select Flow Sample for Subtype</li> <li>■ Select the virtual port vp-hc3scale-4engines-slots1and3 for the Source.</li> <li>■ Select the port group hc3-pg-1 for the Destination.</li> <li>■ Select hc3-scale-fs-lb from the GSOP list.</li> </ul> </li> <li>3. Add a rule. <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select GTP.</li> <li>c. Enter 60 for Percentage.</li> <li>d. Enter 5* in the IMSI field.</li> <li>e. Select V1 for Version</li> </ol> </li> <li>6. Click Save.</li> </ol> |
| 16   | <p>Create a second level map for GTP flow filtering that takes traffic from the virtual port, applies the flow filtering GigaSMART operation, matches IMSIs specified by the flow rule, and sends matching traffic to load balancing port group hc3-q2x32-1-4.</p>                                                                                                                          | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map. <ul style="list-style-type: none"> <li>■ Type from_hc3_ff in the Alias field</li> <li>■ Select Second Level for Type.</li> <li>■ Select Flow Filter for Subtype</li> <li>■ Select the virtual port vp-hc3scale-4engines-slots1and3 for the Source.</li> <li>■ Select the port group hc3-pg-1 for the Destination.</li> <li>■ Select port group hc3-q2x32-1-4 from the GSOP list.</li> </ul> </li> <li>3. Add a rule.</li> </ol>                                                                                                                                                                                                                                  |

| Task | Description                                                                                         | UI Steps                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                                                                                     | <ol style="list-style-type: none"> <li>a. Click Add a Rule.</li> <li>b. Select GTP IMSI</li> <li>c. Enter * in the IMSI field.</li> <li>d. Select Any for Version</li> </ol> <ol style="list-style-type: none"> <li>5. Click Save.</li> </ol>                                                                                                                                                                                                                       |
| 17   | Add a shared collector for any unmatched traffic from the virtual port and send it to a GigaStream. | <ol style="list-style-type: none"> <li>1. Select Maps &gt; Maps &gt; Maps.</li> <li>2. Configure the map. <ul style="list-style-type: none"> <li>■ Type s_coll_hc3 in the Alias field</li> <li>■ Select Second Level for Type.</li> <li>■ Select Collector for Subtype</li> <li>■ Select the virtual port vp-hc3scale-4engines-slots1and3 for the Source.</li> <li>■ Select GigaStream hc3-gs-4 for the Destination.</li> </ul> </li> <li>3. Click Save.</li> </ol> |

## Additional Sources of Information

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

- [How to Download Software and Release Notes from My Gigamon](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VUE Community](#)

## Documentation

©This table lists all the guides provided for GigaVUE-FM, GigaVUE HC Series 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

| GigaVUE-FM, GigaVUE HC Series 6.14.02 Hardware and Software Guides                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>DID YOU KNOW?</b> 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 <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p> |                                                                                                                                                                                                                                    |
| <b>Hardware</b>                                                                                                                                                                                                                                                                                                                     | how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE-FM, GigaVUE HC Series devices; reference information and specifications for the respective GigaVUE-FM, GigaVUE HC Series 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                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                    |
| 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                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                    |

| GigaVUE-FM,GigaVUE HC Series 6.14.02 Hardware and Software Guides                                                  |                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| 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,GigaVUE HC Series 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 HC Series                                                                               |
| 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( <b>NEW</b> ) (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)                                                              |                                                                                                                                       |
| 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                                                        |                                                                                                                                       |

| GigaVUE-FM,GigaVUE HC Series 6.14.02 Hardware and Software Guides                                                                                                                                                                                                              |                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Reference Guides                                                                                                                                                                                                                                                               |                                                                                                                                           |
| <b>GigaVUE-OS CLI Reference Guide</b>                                                                                                                                                                                                                                          | library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices |
| <b>GigaVUE-OS Security Hardening Guide</b>                                                                                                                                                                                                                                     |                                                                                                                                           |
| <b>GigaVUE Firewall and Security Guide</b>                                                                                                                                                                                                                                     |                                                                                                                                           |
| <b>GigaVUE Licensing Guide</b>                                                                                                                                                                                                                                                 |                                                                                                                                           |
| <b>GigaVUE-OS Cabling Quick Reference Guide</b>                                                                                                                                                                                                                                | guidelines for the different types of cables used to connect Gigamon devices                                                              |
| <b>GigaVUE-OS Compatibility and Interoperability Matrix</b>                                                                                                                                                                                                                    | compatibility information and interoperability requirements for Gigamon devices                                                           |
| <b>GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide</b>                                                                                                                                                                                                                | samples uses of the GigaVUE-FM,GigaVUE HC Series Application Program Interfaces (APIs)                                                    |
| <b>Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices</b>                                                                                                                                                                                                          |                                                                                                                                           |
| Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.                                                                                                                                                                                            |                                                                                                                                           |
| Release Notes                                                                                                                                                                                                                                                                  |                                                                                                                                           |
| <b>GigaVUE-OS, GigaVUE-FM,GigaVUE HC Series, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes</b>                                                                                                                                                             | new features, resolved issues, and known issues in this release ;<br>important notes regarding installing and upgrading to this release   |
| <b>Note:</b> Release Notes are not included in the online documentation.                                                                                                                                                                                                       |                                                                                                                                           |
| <b>Note:</b> Registered Customers can log in to <a href="#">My Gigamon</a> to download the Software and Release Notes from the Software and Docs page on to <a href="#">My Gigamon</a> . Refer to <a href="#">How to Download Software and Release Notes from My Gigamon</a> . |                                                                                                                                           |
| In-Product Help                                                                                                                                                                                                                                                                |                                                                                                                                           |
| <b>GigaVUE-FM,GigaVUE HC Series Online Help</b>                                                                                                                                                                                                                                | 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,GigaVUE HC Series" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM,GigaVUE HC Series 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](mailto: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 | (URL for where the issue is)                                                         |
|                             | Topic Heading   | (if it's a long topic, please provide the heading of the section where the issue is) |
|                             |                 |                                                                                      |

|                     |                                                                    |                                                                                                        |
|---------------------|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| For PDF Topics      | Document Title                                                     | (shown on the cover page or in page header )                                                           |
|                     | Product Version                                                    | (shown on the cover page)                                                                              |
|                     | Document Version                                                   | (shown on the cover page)                                                                              |
|                     | Chapter Heading                                                    | (shown in footer)                                                                                      |
|                     | PDF page #                                                         | (shown in footer)                                                                                      |
|                     |                                                                    |                                                                                                        |
| How can we improve? | Describe the issue                                                 | Describe the error or issue in the documentation.<br>(If it helps, attach an image to show the issue.) |
|                     | How can we improve the content?<br><br>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](mailto: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](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

# Premium Support

Email Gigamon at [inside.sales@gigamon.com](mailto: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](https://community.gigamon.com)

**Questions?** Contact our Community team at [community@gigamon.com](mailto: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)